

Security made simple.

SafeGuard Enterprise
Installationsanleitung

Produktversion: 6.1
Stand: Februar 2014

Inhalt

1 Über SafeGuard Enterprise

SafeGuard Enterprise ist eine umfassende, modular aufgebaute Datensicherheitslösung, die Informationen und Informationsaustausch auf Servern, PCs und mobilen Endgeräten durch ein richtlinienbasiertes Verschlüsselungskonzept zuverlässig schützt.

Die zentrale Verwaltung wird im SafeGuard Management Center durchgeführt. Sicherheitsrichtlinien, Schlüssel und Zertifikate, Smartcards und Token können über ein rollenbasiertes Administrationskonzept übersichtlich verwaltet werden. Ausführliche Protokollierung und Reportfunktionen gewährleisten stets den Überblick über alle Ereignisse.

Auf Benutzerseite sind Datenverschlüsselung und Schutz vor Angreifern die primären Sicherheitsfunktionen von SafeGuard Enterprise. SafeGuard Enterprise fügt sich dabei nahtlos in die gewohnte Benutzerumgebung ein und lässt sich leicht und intuitiv bedienen. Die SafeGuard-spezifische Authentisierung, die Power-on Authentication (POA), sorgt für umfassenden Zugriffsschutz und bietet komfortable Unterstützung bei der Wiederherstellung von Anmeldeinformationen.

Hinweis: Einige Features sind nicht in allen Lizenzen enthalten. Für Informationen dazu, was in Ihrer Lizenz enthalten ist, wenden Sie sich an Ihren Vertriebspartner.

1.1 SafeGuard Enterprise Komponenten

Dieser Abschnitt bietet einen Überblick über die SafeGuard Enterprise Komponenten und beschreibt, wie sie zusammenspielen.

Eine oder mehrere Microsoft SQL Datenbanken sammeln Informationen über die Endpoints im Firmennetzwerk. Der Administrator, bei SafeGuard Enterprise heißt er Haupt-Sicherheitsbeauftragter oder Master Security Officer (MSO), nutzt das SafeGuard Management Center, um die Datenbankinhalte zu steuern und neue Sicherheitsrichtlinien (Policies) zu erstellen.

Die Endpoints der Benutzer lesen die Richtlinien aus der Datenbank und berichten die erfolgreiche Ausführung an die Datenbank. Die Kommunikation zwischen Datenbank und Endpoints übernimmt dabei ein Internet Information Services (IIS) basierter Webserver, auf dem der SafeGuard Enterprise Server eingerichtet ist.

SafeGuard Enterprise Komponenten

Die folgende Tabelle beschreibt die einzelnen Komponenten:

Komponente	Beschreibung
SafeGuard Enterprise Datenbank(en) basierend auf Microsoft SQL Server Datenbank	Die SafeGuard Enterprise Datenbank(en) enthält/enthalten alle relevanten Daten wie Schlüssel/Zertifikate, Informationen zu Benutzern und Computern, Ereignisse und die Richtlinieneinstellungen. Zugriff auf die Datenbank(en) benötigt der SafeGuard Enterprise Server und ein einziger Sicherheitsbeauftragter des SafeGuard Management Centers, meist der Haupt-Sicherheitsbeauftragte (MSO). Die Erzeugung und Konfiguration der SafeGuard Enterprise Datenbank(en) kann über einen Assistenten oder über Skripte erfolgen.
SafeGuard Enterprise Server auf IIS basiertem Webserver	Microsoft Internet Information Services (ISS). .NET Framework 4 und ASP.NET 4 sind erforderlich. Der für SafeGuard Enterprise eingesetzte Webserver muss auf Internet Information Services (IIS) basieren. Wir empfehlen den Einsatz eines dedizierten IIS für SafeGuard Enterprise Server.
	Der SafeGuard Enterprise Server ist die Schnittstelle zwischen Datenbank und SafeGuard Enterprise Endpoints. Der SafeGuard Enterprise Server sendet auf Anfrage SafeGuard Enterprise Richtlinieneinstellungen an die Endpoints. Er benötigt Zugriff auf die Datenbank. Er läuft als Anwendung auf einem Microsoft Internet Information Services (IIS) basierten Webserver.
	ASP .NET 4.5 Wenn Sie .NET 4.5 verwenden und SSL als Transportverschlüsselungsmethode für die Client-Server

Komponente	Beschreibung
	Kommunikation wählen, installieren Sie die Rolle *Basic Authentication* zusätzlich zu ASP.NET 4.5.
SafeGuard Management Center auf dem Administratorcomputer	Zentrales Management-Werkzeug für durch SafeGuard Enterprise geschützte Endpoints zur Verwaltung von Schlüsseln und Zertifikaten, Benutzern und Computern, sowie zur Erstellung von SafeGuard Enterprise Richtlinien. Das SafeGuard Management Center kommuniziert mit der SafeGuard Enterprise Datenbank. .NET Framework 4 ist erforderlich.
Verzeichnisdienste (optional)	Import eines Active Directory. Es enthält die Organisationsstruktur des Unternehmens mit Benutzern und Computern.
SafeGuard Enterprise Verschlüsselungssoftware auf Endpoints	Verschlüsselungssoftware zur Authentisierung und Datenverschlüsselung auf Endpoints. Durch SafeGuard Enterprise geschützte Endpoints können entweder mit dem SafeGuard Enterprise Server verbunden sein (zentral verwaltet) oder keine Verbindung zu einem SafeGuard Enteprise Server haben (Standalone). Zentral verwaltete Endpoints erhalten ihre Richtlinien direkt vom SafeGuard Enterprise Server. Standalone-Endpoints erhalten ihre Richtlinien in Konfigurationspaketen, die mit einen Dritt-Verteilungsmechanismus verteilt werden können.

2 Erste Schritte

Dieser Abschnitt erklärt die notwendigen Vorbereitungsmaßnahmen für eine erfolgreiche Installation von SafeGuard Enterprise.

- Erstinstallation: Der SGN Install Advisor vereinfacht die erstmalige Einrichtung der Management-Komponenten einschließlich Standardrichtlinien. Um den SGN Install Advisor für neue SafeGuard Enterprise Installationen aufzurufen, starten Sie **`SGNInstallAdvisor.bat`** aus Ihrer Produktlieferung. Ein Assistent führt Sie durch die Installation.
- Aktualisierung: Führen Sie die in dieser Anleitung beschriebenen Schritte durch.

Hinweis: Nutzen Sie auch die Möglichkeit, SafeGuard Enterprise über Video-Tutorials kennen zu lernen. Sie zeigen die Installation von SafeGuard Enterprise und stellen die Arbeit mit dem SafeGuard Management Center vor. Weitere Informationen finden Sie auf unserer Webseite unter *http://www.sophos.com/de-de/*.

2.1 Installationschritte

Um SafeGuard Enterprise zu installieren, führen Sie die beschriebenen Installationsschritte durch.

Hinweis: SafeGuard Enterprise for Windows unterstützt keine Apple Hardware und kann nicht in einer Boot Camp Umgebung installiert werden.

Alle SafeGuard Enterprise Komponenten (.msi-Pakete) finden Sie in der Produktlieferung.

Schritt	Beschreibung	Paket/Tool
1	Laden Sie die Installer herunter.	
2	Installieren Sie .NET Framework 4 mit ASP.NET 4. Wenn Sie .NET 4.5 verwenden und SSL als Transportverschlüsselungsmethode für die Client-Server Kommunikation wählen wollen, installieren Sie die Rolle *Basic Authentication* zusätzlich zu ASP.NET 4.5.	
3	Richten Sie Internet Information Services (IIS) für die Anwendung mit SafeGuard Enterprise ein.	
4	Installieren Sie SafeGuard Enterprise Server	SGNServer.msi

Schritt	Beschreibung	Paket/Tool
5	Konfigurieren Sie die Microsft SQL Server Authentisierung für den SafeGuard Enterprise Haupt-Sicherheitsbeauftragten.	
6	SafeGuard Enterprise Datenbank(en) über Skripte erzeugen.	Datenbank-Skripte im Verzeichnis Tools\Database Scripts der Produktlieferung
7	Installieren Sie die Management-Konsole SafeGuard Management Center für die zentrale Verwaltung von Benutzern, Computern, Richtlinien, Schlüsseln und Berichten.	SGNManagementCenter.msi
8	Konfigurieren Sie das SafeGuard Management Center: Datenbank und Datenbankserver-Verbindungen, Zertifikate, Anmeldeinformationen für den Haupt-Sicherheitsbeauftragten.	SafeGuard Management Center Konfigurationsassistent
9	Registrieren und konfigurieren Sie den SafeGuard Enterprise Server: Erzeugen Sie das Server-Konfigurationspaket und installieren SIe es auf dem IIS Server.	Konfigurationspakete-Funktion im SafeGuard Management Center.
10	Erstellen Sie die Organisationsstruktur aus Active Directory oder manuell.	SafeGuard Management Center
11	Vorbereiten der Endpoints für die Verschlüsselung	SGxClientPreinstall.msi
12	Erstellen Sie das erste Konfigurationspaket für die Endpoint-Konfiguration.	Konfigurationspakete-Funktion im SafeGuard Management Center.
13	Installieren Sie die Verschlüsselungssoftware und das Konfigurationspaket auf den Endpoints.	Für Informationen zu den verfügbaren Paketen, siehe *Zentral verwaltete Endpoints und Standalone-Endpoints* (Seite 49).

2.2 Handlungsschritte für Runtime-Systeme

Ein Runtime-System ermöglicht das Booten von einem sekundären Boot-Laufwerk, wenn mehrere Betriebssysteme installiert sind und erlaubt den Zugriff auf diese Laufwerke, wenn diese durch eine SafeGuard Enterprise Installation auf dem primären Volume verschlüsselt sind.

Diese Lösung steht sowohl für zentral verwaltete Endpoints als auch für Standalone-Endpoints, die durch SafeGuard Enterprise geschützt sind, zur Verfügung.

Hinweis: SafeGuard Enterprise for Windows unterstützt keine Apple Hardware und kann nicht in einer Boot Camp Umgebung installiert werden.

To install SafeGuard Enterprise encryption software on endpoints with multiple operating systems, follow these installation steps:

Schritt	Beschreibung	Paket/Tool
1	Laden Sie die Installer herunter.	
2	Richten Sie das Runtime-System auf dem sekundären Boot-Laufwerk des Endpoint ein.	SGNClientRuntime.msi, SGNClientRuntime_x64.msi
3	Statten Sie die Endpoints mit notwendigen Voraussetzungen für eine erfolgreiche Installation der aktuellen Verschlüsselungssoftware aus.	SGxClientPreinstall.msi
4	Installieren Sie das SafeGuard Festplattenverschlüsselungs-Paket auf dem primären Boot-Laufwerk des Endpoint.	SGNClient.msi, SGNClient_x64.msi
5	Erstellen Sie das erste Konfigurationspaket für die Endpoint-Konfiguration.	Konfigurationspakete-Funktion im SafeGuard Management Center.

2.3 Überprüfen der Systemanforderungen

Bevor Sie SafeGuard Enterprise installieren, prüfen Sie die Systemanforderungen.

Informationen zu Hardware- und Software-Anforderungen, Service Packs sowie Festplattenspeicherbedarf für Installation und effektiven Betrieb finden Sie in den aktuellen Versionsinfos auf der SafeGuard Versionsinfos Landing-Page *http://www.sophos.com/de-de/support/knowledgebase/112776.aspx*.

2.4 Installer Download

1. Laden Sie die Installer von der Sophos Website herunter. Sie erhalten hierzu von Ihrem Systemadministrator die entsprechende Web-Adresse und die erforderlichen Download-Anmeldeinformationen.
2. Legen Sie die Dateien an einem Speicherort ab, auf den Sie für die Installation Zugriff haben.

2.5 Sprache der Benutzeroberfläche

Die Spracheinstellungen für die Installations- und Konfigurationsassistenten und die verschiedenen SafeGuard Enterprise Komponenten sind wie folgt:

Assistenten

Die Sprache der Installations- und Konfigurationsassistenten der verschiedenen Installationspakete wird automatisch an die Spracheinstellungen des Betriebssystems angepasst. Wenn die Betriebssystemsprache für diese Assistenten nicht verfügbar ist, wird automatisch Englisch benutzt.

SafeGuard Management Center

So stellen Sie die Sprache das SafeGuard Management Center ein:

- Klicken Sie im SafeGuard Management Center auf **Extras** > **Optionen** > **Allgemein**. Klicken Sie auf **Benutzerdefinierte Sprache verwenden** und wählen Sie eine verfügbare Sprache aus. Die Sprachen Englisch, Deutsch, Französisch und Japanisch sind verfügbar.
- Starten Sie das SafeGuard Management Centers neu. Er wird in der ausgewählten Sprache angezeigt.

Sophos SafeGuard auf Endpoints

Die Sprache von Sophos SafeGuard auf Endpoints steuern Sie über den Richtlinientyp **Allgemeine Einstellungen** im SafeGuard Management Center (Einstellung **Anpassung** > **Sprache am Client**):

- Wenn die Sprache des Betriebssystems gewählt wird, richtet sich die Produktsprache nach der Spracheinstellung des Betriebssystems. Steht die entsprechende Betriebssystemsprache in Sophos SafeGuard nicht zur Verfügung, wird standardmäßig die englische Version von Sophos SafeGuard angezeigt.
- Wenn eine der zur Verfügung stehenden Sprachen gewählt wird, werden die Sophos SafeGuard Funktionen auf dem Endpoint in der ausgewählten Sprache angezeigt.

2.6 Kompatibilität mit weiteren SafeGuard-Produkten

Dieser Abschnitt beschreibt die Kompatibilität von SafeGuard Enterprise 6,1 mit anderen SafeGuard-Produkten.

2.6.1 Kompatibilität mit SafeGuard LAN Crypt

SafeGuard LAN Crypt 3.7x und Sophos SafeGuard 6.1 können zusammen auf einem Endpoint installiert werden. Wenn Sie das Feature SafeGuard Data Exchange nutzen möchten, müssen Sie eine zusätzliche Kompatibiliätskomponente für den erfolgreichen Betrieb dieser Produktversionen auf einem Endpoint installieren.

Hinweis: Sie finden die Kompatibiliätskomponente in Ihrer Produktlieferung. Installieren Sie `SGFileEncCompLayer.msi` auf 32-Bit-Systemen und `SGFileEncCompLayer_x64.msi` auf 64-Bit-Systemen.

SafeGuard LAN Crypt 3.7x ist bereits installiert:

1. Installieren Sie die Kompatibilitätskomponente auf dem Endpoint.
2. Installieren Sie das SafeGuard Prä-Installationspaket auf dem Endpoint.
3. Installieren Sie SafeGuard Data Exchange auf dem Endpoint.
4. Installieren Sie das SafeGuard-Client-Konfigurationspaket auf dem Endpoint.
5. Starten Sie den Endpoint neu.

Hinweis: Während der Installation wird unter Umständen eine Meldung angezeigt, die Sie darüber informiert, dass die Komponente SGLC Profile Loader bereits in Gebrauch ist. Sie können diese Meldung ignorieren. Sie wird dadurch verursacht, dass SafeGuard LAN Crypt und SafeGuard Enterprise gemeinsame Komponenten benutzen. Die betroffenen Komponenten werden beim Neustart aktualisiert.

SafeGuard Enterprise 6.1 ist bereits installiert:

1. Installieren Sie SafeGuard LAN Crypt 3.7x auf dem Endpoint.
2. Installieren Sie die Kompatibiliätskomponente auf dem Endpoint.
3. Starten Sie den Endpoint neu.

Hinweis: Frühere Versionen beider Produkte können nicht zusammen auf einem Computer installiert werden. Wenn Sie zum Beispiel versuchen, SafeGuard LAN Crypt 3.6x auf einem Computer zu installieren, auf dem bereits SafeGuard Enterprise 6.1 installiert ist, wird die Installation mit einer Fehlermeldung abgebrochen.

2.6.2 Kompatibilität mit SafeGuard PrivateCrypto und SafeGuard PrivateDisk

SafeGuard Enterprise 6,1 und die Standalone Produkte SafeGuard PrivateCrypto ab Version 2.30 sowie SafeGuard PrivateDisk ab Version 2.30 können gleichzeitig auf einem Computer installiert sein.

Sowohl SafeGuard PrivateCrypto als auch SafeGuard PrivateDisk können dann das SafeGuard Enterprise Schlüsselmanagement mit benutzen.

2.6.3 Kompatibilität mit SafeGuard RemovableMedia

Die Komponente SafeGuard Data Exchange und SafeGuard RemovableMedia können nicht zusammen auf einem Computer installiert werden. Bevor Sie das SafeGuard Data Exchange auf einem Endpoint installieren, prüfen Sie, ob SafeGuard RemovableMedia bereits installiert

ist. In diesem Fall müssen Sie SafeGuard RemovableMedia deinstallieren, bevor Sie SafeGuard Data Exchange installieren.

Lokale Schlüssel, die vor dem Wechsel zu SafeGuard Data Exchange mit einer SafeGuard RemovableMedia Version vor 1.20 erzeugt wurden, können auf durch SafeGuard Enterprise geschützte Computer benutzt werden. Sie werden jedoch nicht automatisch an die SafeGuard Enterprise Datenbank übertragen.

2.7 Allgemeine Einschränkungen

Beachten Sie folgende allgemeine Einschränkungen für SafeGuard Enterprise auf Endpoints:

- SafeGuard Enterprise for Windows unterstützt keine Apple Hardware und kann nicht in einer Boot Camp Umgebung installiert werden.
- Wenn auf dem Endpoint Intel Advanced Host Controller Interface (AHCI) benutzt wird, muss sich die Boot-Festplatte in Slot 0 oder Slot 1 befinden. Sie können bis zu 32 Festplatten einlegen. SafeGuard Enterprise läuft nur auf den ersten beiden Slot-Nummern.
- SafeGuard volume-basierende Verschlüsselung für Volumes, die sich auf dynamischen Datenträgern oder auf GUID Partitionstabellen (GPT)-Platten befinden, wird nicht unterstützt. Die Installation bricht in diesen Fällen ab. Wenn diese Platten auf dem Endpoint gefunden werden, werden sie nicht unterstützt.
- Systeme mit Festplatten, die über einen SCSI Bus angeschlossen sind, werden von der Sophos SafeGuard Festplattenverschlüsselung nicht unterstützt.
- Der **schnelle Benutzerwechsel** wird nicht unterstützt.
- Der Einsatz von SafeGuard Enterprise in einer Terminal Server Umgebung wird nicht unterstützt.

3 Einrichten des SafeGuard Enterprise Servers

Der SafeGuard Enterprise Server stellt die Schnittstelle zu den SafeGuard Enterprise Clients her. Er greift wie das SafeGuard Management Center auf die Datenbank zu. Er läuft als Applikation auf einem Web Server basierend auf Microsoft Internet Information Services (IIS).

Der SafeGuard Enterprise Server bietet außerdem den Taskplaner, mit dem Sie periodische Tasks, die auf Skripten basieren, erstellen und geplant ausführen lassen können. Die Tasks laufen automatisch auf dem SafeGuard Enterprise Server. Sie finden die Skripte in der SafeGuard Enterprise Produktlieferung. Weitere Informationen hierzu finden Sie in der *SafeGuard Enterprise Administratorhilfe*.

Wir empfehlen den Einsatz eines dedizierten IIS für SafeGuard Enterprise Server. Dadurch wird die Performance verbessert. Außerdem verhindert dies, dass andere Anwendungen mit SafeGuard Enterprise in Konflikt geraten, z. B. wegen der verwendeten Version von ASP.NET.

Dieses Kapitel beschreibt, wie Sie SafeGuard Enterprise Server mit Taskplaner auf IIS installieren. Zuerst müssen Sie Microsoft Internet Information Services (IIS) installieren und konfigurieren.

3.1 Voraussetzungen

Folgende Voraussetzungen müssen erfüllt sein:

- Sie benötigen Windows Administratorrechte.
- Microsoft Internet Information Services (IIS) muss verfügbar sein.

  IIS ist kostenlos verfügbar. Sie finden das Programm z. B. auf Ihrer Windows-DVD oder auf der Microsoft Website.

- Wenn Sie SSL als Transportverschlüsselung zwischen SafeGuard Enterprise Server und SafeGuard Enterprise Client verwenden, muss der IIS Server dafür eingerichtet werden, siehe *Sichern von Transportverbindungen mit SSL* (Seite 40).

    Ein Zertifikat muss ausgestellt und der IIS Server so konfiguriert werden, dass er SSL verwendet und auf das Zertifikat zeigt.
    Der Servername, den Sie bei der Konfiguration des SafeGuard Enterprise Servers angeben, muss identisch sein mit dem Servernamen, den Sie vorab im SSL-Zertifikat angegeben haben. Sonst können Client und Server nicht miteinander kommunizieren. Für jeden SafeGuard Enterprise Server wird ein separates SSL-Zertifikat benötigt.
    Wenn Sie Network Load Balancer einsetzen, vergewissern Sie sich, dass der Portbereich den SSL-Port mit einschließt.

- .NET Framework 4 und ASP.NET 4 muss installiert sein. Das Programm steht in der SafeGuard Enterprise Produktlieferung zur Verfügung.

3.2 Installation und Konfiguration von Microsoft Internet Information Services (IIS)

Dieser Abschnitt beschreibt, wie Sie Microsoft Internet Information Services (IIS) für den Betrieb mit SafeGuard Enterprise Server vorbereiten.

3.2.1 Installieren und Konfigurieren von IIS 7/7.5 auf Microsoft Windows Server 2008/2008 R2

IIS ist kostenlos verfügbar. Sie finden das Programm z. B. auf Ihrer Windows-DVD oder auf der Microsoft Website.

1. Klicken Sie im **Start** Menü auf **Alle Programme**, **Administration** und dann auf **Server-Manager**.
2. Klicken Sie im **Server Manager** auf **Rollenübersicht** und klicken Sie dann auf **Rollen hinzufügen**.
3. Verifizieren Sie auf der **Vorbemerkungen** Seite des **Rollen hinzufügen** Assistenten Folgendes:
   - Das Administratorenkonto hat ein sicheres Kennwort.
   - Die Netzwerkeinstellungen, z. B. IP-Adressen, sind konfiguriert.
   - Die neuesten Windows-Sicherheits-Updates sind installiert.
4. Wählen Sie **Rollen auswählen** auf der rechten Seite und dann **Webserver (IIS)**. Klicken Sie auf der folgenden Seite auf **Erforderliche Features hinzufügen** Seite. **Webserver (IIS)** ist im Navigationsbereich des **Rollen hinzufügen** Assistenten aufgelistet.
5. Klicken Sie auf **Webserver (IIS)** und dann auf **Rollendienste**. Behalten Sie die Standard-Rollendienste bei.
6. Wählen Sie auf der rechten Seite zusätzlich Folgendes: **ASP.NET**, dadurch werden alle notwendigen untergeordneten Rollendienste ebenfalls ausgewählt.
7. Wählen Sie **IIS Management Scripts and Tools**. Dies ist für die richtige IIS 7 Konfiguration erforderlich.
8. Klicken Sie auf **Weiter**, dann auf **Installieren** und dann auf **Schließen**,

   IIS wird mit einer Standardkonfiguration zum Hosten von ASP.NET installiert.

9. Überprüfen Sie mit http://< server name>, ob die Web-Seite korrekt angezeigt wird. Weitere Informationen finden Sie unter: *http://support.microsoft.com*.

3.2.1.1 Prüfen der .NET Framework Registrierung bei IIS 7

.NET Framework Version 4 ist erforderlich.

1. Um zu überprüfen, ob .NET Framework installiert und mit der korrekten Version registriert ist, siehe *Prüfen der .NET Framework Installation und Registrierung*.

3.2.1.2 Prüfen der ASP.NET Registrierung bei IIS 7

ASP.NET Version 4 ist erforderlich.

1. Um zu überprüfen, ob ASP.NET installiert und mit der korrekten Version registriert ist, geben Sie das Kommando **aspnet_regiis.exe -lv** auf der Kommandozeile ein.

Für ASP.NET Version sollte Version 4.0 angezeigt werden.

3.2.2 Installieren und Konfigurieren von IIS 8 auf Microsoft Windows Server 2012/2012 R2

IIS ist kostenlos verfügbar. Sie finden das Programm z. B. auf Ihrer Windows-DVD oder auf der Microsoft Website.

1. Am **Server-ManagerDashboard**, klicken Sie auf **Verwalten** und wählen Sie **Rollen und Features hinzufügen**.
2. Im **Assistent zum Hinzufügen von Rollen und Features**, auf der Seite **Vorbemerkungen**, überprüfen Sie Folgendes:
   - Das Administratorenkonto hat ein sicheres Kennwort.
   - Die Netzwerkeinstellungen, z. B. IP-Adressen, sind konfiguriert.
   - Die neuesten Windows-Sicherheits-Updates sind installiert.
3. Wählen Sie **Serverrollen** im linken Fenster und wählen Sie dann **Web Server (IIS)**. Klicken Sie auf **Features hinzufügen** im angezeigten Fenster. **Rolle "Webserver" (IIS)** wird im linken Bereich des **Assistent zum Hinzufügen von Rollen und Features** gelistet.
4. Wählen Sie **Rollendienste** unter **Rolle "Webserver" (IIS)**. Behalten Sie die Standard-Rollendienste bei.
5. Scrollen Sie nach unten zum Knoten **Application Development** und aktivieren Sie:
   - **ASP.NET 4.5**
   - **ISAPI Extensions**
   - **ISAPI Filters**

   Notwendige untergeordnete Rollendienste werden automatisch ausgewählt.
6. Unter dem Knoten **Security** aktivieren Sie:
   - **Basic Authentication**
   - **Windows Authentication**
7. Klicken Sie auf **Weiter**, dann **Installieren** and **Schließen**,

   Ihr IIS Serverdienst ist nun mit einer Standardkonfiguration zum Hosten von ASP.NET installiert.

3.3 Installieren von SafeGuard Enterprise Server

Nachdem der IIS konfiguriert ist, können Sie SafeGuard Enterprise Server auf dem IIS Server installieren. Das Installationspaket **`SGNServer.msi`** finden Sie in der Produktlieferung.

1. Doppelklicken Sie auf dem Server, auf dem Sie SafeGuard Enterprise Server installieren möchten, auf **`SGNServer.msi`**. Ein Assistent führt Sie durch die notwendigen Schritte.
2. Übernehmen Sie in den folgenden Dialogen die Standardeinstellungen. Der Taskplaner wird automatisch mit dem Installationstyp **Vollständig** installiert.

SafeGuard Enterprise Server mit Taskplaner wird installiert.

Hinweis: Aus Performance-Gründen ist die Verkettung von protokollierten Ereignissen für die SafeGuard Enterprise Datenbank nach der Installation des SafeGuard Enterprise Servers standardmäßig deaktiviert. Ohne die Verkettung steht für die protokollierten Ereignisse jedoch kein Integritätsschutz zur Verfügung. Die Verkettung verknüpft alle Einträge in der Ereignistabelle miteinander, so dass die Entfernung eines Eintrags sichtbar wird und über eine Integritätsprüfung nachgewiesen werden kann. Um den Integritätsschutz zu nutzen, müssen Sie die Verkettung von protokollierten Ereignissen manuell aktivieren. Detaillierte Informationen hierzu finden Sie im Kapitel *Berichte* der *SafeGuard Enterprise Administrator-Hilfe*.

4 Einrichten einer SafeGuard Enterprise Datenbank

SafeGuard Enterprise speichert alle relevanten Daten wie Schlüssel/Zertifikate, Informationen zu Benutzern und Computern, Ereignisse und die Richtlinieneinstellungen in einer Datenbank. Die SafeGuard Enterprise Datenbank basiert auf Microsoft SQL Server.

Prüfen Sie die Liste der aktuell unterstützten SQL Server Typen im Abschnitt zu den Systemanforderungen in den aktuellen Versionsinfos unter *http://www.sophos.com/de-de/support/knowledgebase/112776.aspx*.

Sie können die Datenbank entweder automatisch während der Erstkonfiguration im SafeGuard Management Center oder manuell mit den in Ihrer Produktlieferung verfügbaren SQL Skripten einrichten. Wählen Sie die geeignete Methode nach den Gegebenheiten in Ihrer Firmenumgebung. Für weitere Informationen, siehe *Datenbankzugriffsrechte* (Seite 17).

Zur Optimierung der Performance lässt sich die SafeGuard Enterprise Datenbank auf mehrere SQL Server replizieren. Für Informationen zum Einrichten der Datenbankreplikation, siehe *Replikation der SafeGuard Enterprise Datenbank* (Seite 74).

Sie können mehrere SafeGuard Enterprise Datenbanken für unterschiedliche Mandanten, z. B. Firmenstandorte, Organisationseinheiten oder Domänen, einrichten und verwalten. Für Informationen zur Konfiguration von Multi Tenancy, siehe *Multi Tenancy Konfigurationen* (Seite 27).

Hinweis: Wir empfehlen den Einsatz eines permanenten Online-Backups für die Datenbank. Führen Sie ein regelmäßiges Backup Ihrer Datenbank durch, um Schlüssel, Unternehmenszertifikate und Benutzer-Computer-Zuordnungen zu sichern. Beispiele für empfohlene Backup-Zyklen: nach dem Erstimport der Daten, nach größeren Änderungen oder in turnusmäßigen Abständen, z. B. wöchentlich oder täglich.

4.1 Datenbank-Authentisierung

Um auf die SafeGuard Enterprise Datenbank zuzugreifen, muss sich der erste Sicherheitsbeauftragte des SafeGuard Management Centers am SQL Server authentisieren. Es gibt folgende Möglichkeiten:

- Windows-Authentisierung: Ernennen Sie einen vorhandenen Windows-Benutzer zum SQL-Benutzer
- SQL-Authentisierung: Richten Sie ein SQL-Benutzerkonto ein.

Fragen Sie Ihren SQL-Administrator, welche Form der Authentisierung für Sie als Sicherheitsbeauftragter vorgesehen ist. Sie benötigen diese Information vor der Erzeugung der Datenbank und vor der Erstkonfiguration des SafeGuard Management Centers im SafeGuard Management Center Konfigurationsassistenten.

Verwenden Sie SQL-Authentisierung für Computer, die sich nicht in einer Domäne befinden. Ansonsten verwenden Sie Windows-Authentisierung. Wenn Sie SQL-Authentisierung einsetzen, empfehlen wir, die Verbindung zu und vom Datenbankserver durch SSL zu sichern. Für weitere Informationen, siehe *Einrichten von SSL* (Seite 40).

4.1.1 Datenbankzugriffsrechte

SafeGuard Enterprise ist so eingerichtet, dass es für das Zusammenspiel mit der SQL-Datenbank nur ein einziges Benutzerkonto mit minimalen Zugriffsberechtigungen auf die Datenbank benötigt. Dieses Benutzerkonto wird vom SafeGuard Management Center genutzt und lediglich auf den ersten Sicherheitsbeauftragten des SafeGuard Management Centers ausgestellt. Damit ist die Verbindung zur SafeGuard Enterprise Datenbank gewährleistet. Während des Betriebs von SafeGuard Enterprise benötigt ein einziger Sicherheitsbeauftragter des SafeGuard Management Centers nur die Lese/Schreib-Berechtigung für die SafeGuard Enterprise Datenbank.

Die SafeGuard Enterprise Datenbank kann entweder manuell oder automatisch während der Erstkonfiguration im SafeGuard Management Center erzeugt werden. Soll die Datenbank automatisch erstellt werden, so sind für den ersten SafeGuard Management Center Sicherheitsbeauftragten erweiterte Zugriffsrechte für die SQL Datenbank (db_creator) erforderlich. Diese Berechtigungen können dem Sicherheitsbeauftragten danach vom SQL-Administrator aber wieder bis zur nächsten Installation/Aktualisierung entzogen werden.

Wenn die Erweiterung der Rechte während der Installation des SafeGuard Management Centers nicht gewünscht ist, kann der SQL-Administrator die SafeGuard Enterprise Datenbank per Skript erzeugen. Dazu können die beiden Skripte **CreateDatabase.sql** und **CreateTables.sql** aus der Produktlieferung ausgeführt werden.

Die folgende Tabelle zeigt die notwendigen SQL-Berechtigungen für die unterschiedlichen Versionen von Microsoft SQL Server.

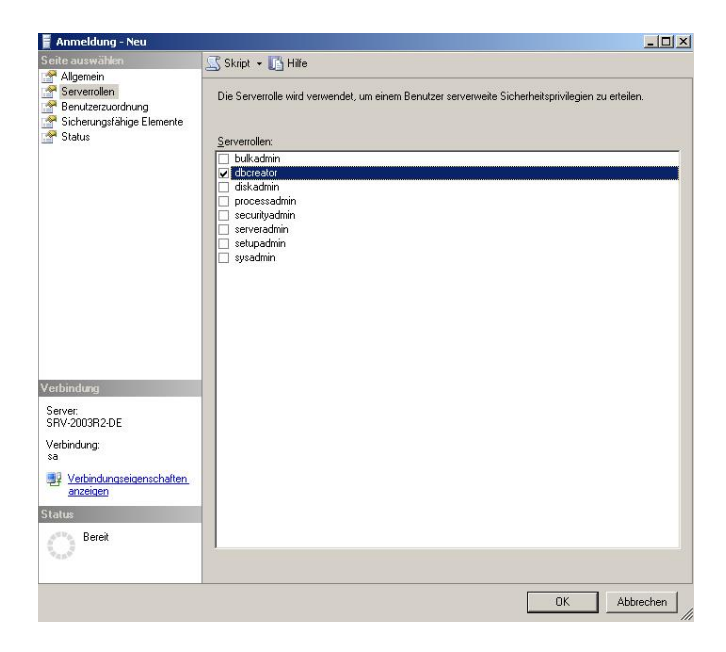
Zugriffsberechtigung	SQL Server 2008, SQL Server 2008 Express
Datenbank erstellen	
Server	db_creator
Master Datenbank	keine
SafeGuard Enterprise Datenbank	db_ownerpublic (Standard)
Datenbank benutzen	
Server	keine
Master Datenbank	keine
SafeGuard Enterprise Datenbank	db_datareader db_datawriter public (Standard)

4.1.2 Konfigurieren eines Windows-Benutzerkontos für die Anmeldung am SQL Server

Die folgende Beschreibung der einzelnen Konfigurationsschritte wendet sich an SQL-Administratoren und bezieht sich auf Microsoft Windows Server 2008 und Microsoft SQL Server 2005, Standard oder Express Edition.

Als SQL-Administrator benötigen Sie das Recht zum Anlegen von Benutzerkonten.

1. Öffnen Sie SQL Server Management Studio. Melden Sie sich am SQL Server mit Ihren Anmeldeinformationen an.
2. Öffnen Sie den **Objekt-Explorer**, klicken Sie mit der rechten Maustaste auf **Sicherheit**, wählen Sie **Neu** und klicken Sie dann auf **Anmeldungen**.
3. Wählen Sie unter **Anmeldung - Neu** auf der **Allgemein** Seite die Option **Windows-Authentifizierung**.
4. Klicken Sie auf **Suchen**. Suchen Sie nach dem relevanten Windows-Benutzernamen und klicken Sie auf **OK**. Der Benutzername wird als **Anmeldename** angezeigt.
5. Wenn noch keine SafeGuard Enterprise Datenbank durch ein Skript angelegt wurde, wählen Sie unter **Standarddatenbank** die Option **Master**.
6. Klicken Sie auf **OK**.
7. Um die Datenbank automatisch während der Erstkonfiguration des SafeGuard Management Centers zu erzeugen, müssen Sie die Zugriffsrechte wie folgt ändern: Weisen Sie jetzt unter **Anmeldung - Neu** die Zugangsberechtigungen/Rollen zu, indem Sie links auf **Serverrollen** klicken: Wählen Sie **dbcreator**. Nach der Installation von SafeGuard Enterprise kann die Datenbankrolle auf **dbowner** zurückgesetzt werden.



4.1.3 Erstellen eines SQL-Kontos für die Anmeldung am SQL Server

Die nachfolgende Beschreibung der einzelnen Konfigurationsschritte richtet sich an SQL-Administratoren. Sie bezieht sich auf Microsoft Windows Server 2008 mit Microsoft SQL Server 2008 Standard Edition.

Als SQL-Administrator benötigen Sie das Recht, ein SQL-Benutzerkonto zu erstellen.

1. Öffnen Sie SQL Server Management Studio. Melden Sie sich am SQL Server mit Ihren Anmeldeinformationen an.
2. Öffnen Sie den **Objekt-Explorer**, klicken Sie mit der rechten Maustaste auf **Sicherheit**, wählen Sie **Neu** und klicken Sie dann auf **Anmeldungen**.
3. Wählen Sie unter **Anmeldung - Neu** auf der **Allgemein** Seite die Option **SQL Server Authentifizierung**.
4. Führen Sie auf der **Allgemein** Seite bei **Anmeldename** folgende Schritte durch:

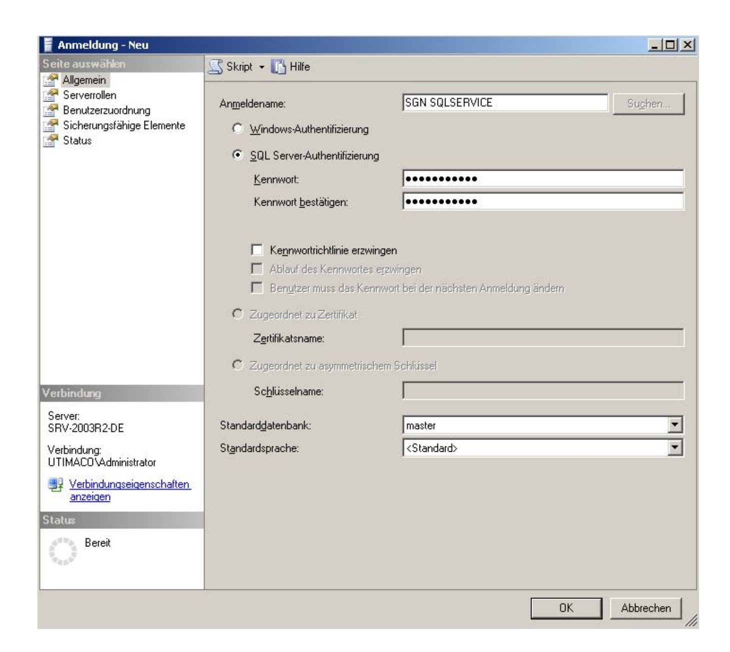
    a) Geben Sie den Namen des neuen Benutzers ein, z. B. SGN SQLSERVICE.

    b) Geben Sie ein Kennwort für das Konto ein und bestätigen Sie es.

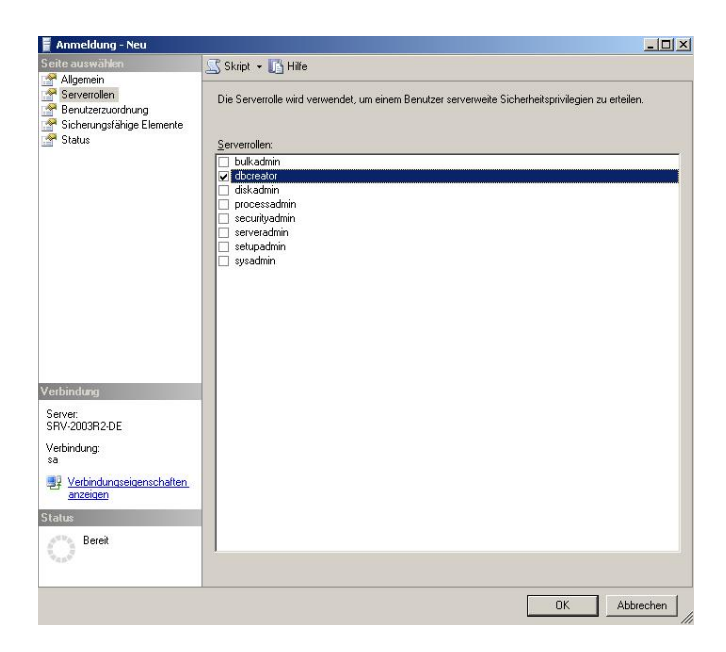
    c) Deaktivieren Sie **Kennwortrichtlinie erzwingen**.

    d) Wenn noch keine SafeGuard Enterprise Datenbank durch ein Skript angelegt wurde, wählen Sie unter **Standarddatenbank** die Option **Master**. Klicken Sie auf **OK**.

    Notieren Sie sich die Authentisierungsmethode und die Anmeldedaten. Sie müssen diese dem SafeGuard Management Center Sicherheitsbeauftragten mitteilen.



5. Um die Datenbank automatisch während der Erstkonfiguration des SafeGuard Management Centers zu erzeugen, müssen Sie die Zugriffsrechte wie folgt ändern: Weisen Sie jetzt unter **Anmeldung - Neu** unter **Allgemein** die Zugangsberechtigungen/Rollen zu, indem Sie links auf **Serverrollen** klicken. Wählen Sie **dbcreator**. Nach der Installation von SafeGuard Enterprise kann die Datenbankrolle auf **dbowner** zurückgesetzt werden.



Das SQL-Benutzerkonto und die Zugriffsberechtigungen sind damit für den SafeGuard Enterprise Sicherheitsbeauftragten eingerichtet.

4.2 Erzeugen der SafeGuard Enterprise Datenbank

Nachdem das Benutzerkonto für die SQL Server Anmeldung eingerichtet ist, können Sie die SafeGuard Enterprise Datenbank erzeugen. Hier gibt es zwei Möglichkeiten:

- Mit dem SafeGuard Management Center Konfigurationsassistenten

  Als Sicherheitsbeauftragter können Sie die SafeGuard Enterprise Datenbank während der Erstkonfiguration im SafeGuard Management Centers leicht und bequem erstellen. Der SafeGuard Management Center Konfigurationsassistent führt Sie durch die Basiskonfiguration, zu der auch die Erstellung der Datenbank gehört. Fahren Sie hierzu mit der Installation und Konfiguration des SafeGuard Management Center fort (siehe *Einrichten des SafeGuard Management Centers* (Seite 25)) und ändern Sie dann die relevanten Zugriffsrechte (siehe *Ändern der Zugriffsrechte für die SafeGuard Enterprise Datenbank* (Seite 22)).

- Mit SQL Skripts, die in der Produktlieferung zur Verfügung stehen.

  Dieser Weg ist dann angebracht, wenn die Erweiterung der Datenbankberechtigung während der Konfiguration des SafeGuard Management Centers nicht gewünscht ist.

Es hängt von Ihrer Unternehmensumgebung ab, welche Methode Sie anwenden. Am besten sollte dies zwischen SQL-Administrator und SafeGuard Enterprise Sicherheitsbeauftragten vorab geklärt werden.

4.2.1 Voraussetzungen

Folgende Voraussetzungen müssen erfüllt sein:

- Microsoft SQL Server muss bereits installiert und konfiguriert sein. Für kleinere Unternehmen eignet sich der Einsatz der Microsoft SQL Express Edition, da keine Lizenzkosten anfallen.
- Aus Performance-Gründen sollte Microsoft SQL Server nicht auf dem Rechner installiert werden, auf dem der SafeGuard Enterprise Server installiert wird.
- Die Authentisierungsverfahren sowie die Zugriffsrechte für die Datenbank sollten geklärt werden.

4.2.2 Erzeugen der SafeGuard Enterprise Datenbank per Skript

Wenn Sie die SafeGuard Datenbank automatisch während der Konfiguration des SafeGuard Management Center erzeugen möchten, können Sie diesen Schritt überspringen. Wenn erweiterte SQL-Berechtigungen während der SafeGuard Management Center Konfiguration nicht erwünscht sind, führen Sie diesen Schritt aus. Dazu stehen im Tools-Verzeichnis der Produktlieferung zwei Datenbank-Skripte zur Verfügung:

- CreateDatabase.sql
- CreateTables.sql

Die folgende Beschreibung der Arbeitsschritte wendet sich an SQL-Administratoren und bezieht sich auf Microsoft SQL Server 2008 Standard Edition.

Als SQL-Administrator benötigen Sie das Recht zum Erstellen einer Datenbank.

1. Kopieren Sie die Skripte CreateDatabase.sql und CreateTables.sql aus der SafeGuard Enterprise Produktlieferung auf den SQL Server.
2. Doppelklicken Sie auf dem Skript **CreateDatabase.sql**. Das Programm SQL Server Management Studio wird aufgerufen.
3. Melden Sie sich am SQL Server mit Ihren Anmeldeinformationen an.
4. Überprüfen Sie, ob die beiden Zielpfade, die zu Beginn des Skripts unter **FILENAME** (MDF, LDF) angegeben sind, auf der lokalen Festplatte vorhanden sind. Korrigieren Sie sie, wenn nötig.
5. Klicken Sie auf die Schaltfläche **Ausführen** in der Symbolleiste, um die Datenbank zu erzeugen. Sie haben die Datenbank **SafeGuard** angelegt. Erzeugen Sie anschließend die Tabellen mit Hilfe des Skripts CreateTables.sql aus der Produktlieferung.
6. Doppelklicken Sie auf **CreateTables.sql**. Ein weiterer Bereich wird in Microsoft SQL Server Management Studio geöffnet.
7. Geben Sie am Beginn des Skripts **`use SafeGuard`** ein, um die SafeGuard Enterprise Datenbank auszuwählen, in der die Tabellen erstellt werden sollen.

8. Klicken Sie auf die Schaltfläche **Ausführen** in der Symbolleiste, um die Tabellen zu erzeugen.

Die SafeGuard Enterprise Datenbank und die zugehörigen Tabellen sind erzeugt.

4.3 Ändern der Zugriffsrechte für die SafeGuard Enterprise Datenbank

Nach dem Erstellen der SafeGuard Enterprise Datenbank, entweder per Skript oder im SafeGuard Management Center, können die Zugriffsrechte wieder geändert werden. Da es möglich ist, einem Benutzer für eine Datenbank unterschiedliche Rollen und Berechtigungen zuzuweisen, sind nur die Mindestrechte für die Herstellung einer Verbindung zur SafeGuard Enterprise Datenbank erforderlich.

1. Öffnen Sie SQL Server Management Studio. Melden Sie sich am SQL Server mit Ihren Anmeldeinformationen an.
2. Öffnen Sie den **Objekt-Explorer**, doppelklicken Sie auf **Sicherheit** und dann auf **Anmeldungen**.
3. Klicken Sie mit der rechten Maustaste auf den erforderlichen Benutzer und klicken Sie dann auf **Eigenschaften**.
4. Wählen Sie **Benutzerzuordnung** auf der linken Seite. Wählen Sie unter **Users mapped to this login** (**Benutzer, die dieser Anmeldung zugeordnet sind**) die Datenbank **SafeGuard**.
5. Stellen Sie unter **Database role membership for** (**Datenbankrollenmitgliedschaft für**) die Zugriffsrechte für die Benutzung der SafeGuard Enterprise Datenbank ein: wählen Sie **db_datareader**, **db_datawriter** und **public**.
6. Klicken Sie auf **OK**.

4.4 Überprüfung von Einstellungen für SQL-Dienste, Named Pipes und TCP/IP

Diese Beschreibung bezieht sich auf Microsoft Windows Server 2008 (R2) und Microsoft SQL Server 2008 Standard oder Express Edition.

1. Öffnen Sie den SQL Server-Konfigurations-Manager.
2. Wählen Sie in der Navigationsstruktur auf der linken Seite **SQL Server-Dienste**.
3. Überprüfen Sie, ob der **Status** von **SQL Server** und **SQL Server Browser Läuft** und der **Startmodus** auf **Automatisch** eingestellt ist.
4. Wählen Sie in der Navigationsstruktur auf der linken Seite **SQL Server-Netzwerkkonfiguration**.
5. Klicken Sie mit der rechten Maustaste auf das Protokoll **Named Pipes** und klicken Sie auf **Aktiviert**.
6. Klicken Sie mit der rechten Maustaste auf das Protokoll **TCP/IP** und klicken Sie auf **Aktiviert**.
7. Klicken Sie außerdem mit der rechten Maustaste auf das Protokoll **TCP/IP** und klicken Sie auf **Eigenschaften**. Belassen Sie in der Registerkarte **IP-Adressen** unter **IPAlll** das Feld **Dynamische TCP-Ports** leer. Geben Sie im Feld **TCP Port** 1433 ein.
8. Starten Sie die SQL-Dienste neu.

4.5 Erstellen einer Windows Firewall Regel auf Windows Server 2008 (R2)

Diese Beschreibung bezieht sich auf Microsoft Windows Server 2008 (R2) mit Microsoft SQL Server 2008 Standard oder Express Edition. Wenn Sie diese Konfiguration verwenden, führen Sie die nachfolgend angegebenen Schritte aus um sicherzustellen, dass eine Verbindung zwischen der SafeGuard Enterprise Datenbank und dem SafeGuard Management Center hergestellt werden kann.

1. Klicken Sie auf dem Computer, der als Host für die SQL Server Instanz dient, auf **Start**, wählen Sie **Verwaltung** und klicken Sie dann auf **Windows-Firewall mit erweiterter Sicherheit**.
2. Wählen Sie in der Navigationsstruktur auf der linken Seite **Eingehende Regeln**.
3. Klicken Sie in der Menüleiste auf **Aktion** und dann auf **Neue Regel** Der **Assistent für neue eingehende Regeln** wird gestartet.
4. Wählen Sie auf der **Regeltyp** Seite **Benutzerdefiniert** und klicken Sie auf **Weiter**.
5. Wählen Sie auf der **Programm** Seite die Programme und Dienste, auf die diese Regel angewendet werden soll. Klicken Sie dann auf **Weiter**.
6. Wählen Sie auf der **Protokolle und Ports** Seite **TCP** als **Protokolltyp**. Wählen Sie für **Lokaler Port** die Option **Bestimmte Ports** und geben Sie **1433** ein. Wählen Sie für **Remoteport** die Option **Alle Ports**. Klicken Sie auf **Weiter**.
7. Auf der **Bereich** Seite können Sie festlegen, dass die Regel nur für den Netzverkehr von oder an die auf dieser Seite angegebenen IP-Adressen gilt. Nehmen Sie die entsprechende Konfiguration vor und klicken Sie auf **Weiter**.
8. Wählen Sie auf der Seite **Aktion** die Option **Verbindung zulassen** und klicken Sie auf **Weiter**.
9. Geben Sie auf der Seite **Profil** an, wo die Regel angewendet werden soll. Klicken Sie dann auf **Weiter**.
10. Geben Sie auf der Seite **Name** einen Namen und eine Beschreibung für Ihre Regel ein und klicken Sie auf **Beenden**.

4.6 Konfigurieren der Windows-Authentisierung für die Anmeldung am SQL Server

Diese Beschreibung bezieht sich auf Microsoft Windows Server 2008 mit Microsoft SQL Server 2008 Standard Edition und IIS 7.

Um die Kommunikation zwischen dem SafeGuard Enterprise Server und der SafeGuard Enterprise Datenbank bei Anwendung der Windows-Authentisierung zu ermöglichen, muss der Benutzer zu einem Mitglied von Active Directory Gruppen gemacht werden. Die Berechtigungen für lokale Dateien müssen angepasst werden und das SQL Benutzerkonto muss in den Anwendungspool des IIS aufgenommen werden.

1. Wählen Sie **Start** und dann **Ausführen**. Geben Sie **dsa.msc** ein. Öffnen Sie das Active Directory Users and Computers Snap-in.

2. Klappen Sie in der Navigationsstruktur auf der linken Seite die Domänenstruktur aus und wählen Sie **Builtin**.
3. Fügen Sie den relevanten Windows-Benutzer zu folgenden Gruppen hinzu: IIS_IUSRS, Performance Log Users, Performance Monitor Users.
4. Beenden Sie das Snap-in.
5. Klicken Sie im lokalen Dateisystem im Windows Explorer mit der rechten Taste auf den C:\Windows\Temp Ordner und wählen Sie **Eigenschaften**. Wählen unter **Eigenschaften** die Registerkarte **Sicherheit**.
6. Klicken Sie unter **Sicherheit** auf **Hinzufügen** und geben Sie den relevanten Windows-Benutzernamen im Feld **Geben Sie die zu verwendenden Objektnamen ein** ein. Klicken Sie auf **OK**.
7. Klicken Sie unter **Sicherheit** bei **Berechtigungen** auf **Erweitert**. Klicken Sie in der **Berechtigungen** Registerkarte des Dialogs **Erweiterte Sicherheitseinstellungen für Temp** auf **Bearbeiten**. Setzen Sie dann im **Objekt** Dialog die folgenden Berechtigungen auf **Zulassen: Ordner auflisten / Daten lesen**, **Dateien erstellen / Daten schreiben**, **Löschen**.
8. Klicken Sie auf **OK**, schließen Sie den Dialog **Eigenschaften für Temp** und schließen Sie dann den Windows Explorer.
9. Öffnen Sie den **Internet Information Services Manager**.
10. Wählen Sie im **Verbindungen** Bereich auf der linken Seite die **Anwendungspools** für den relevanten Server-Knoten.
11. Wählen Sie aus der **Anwendungspools** Liste auf der rechten Seite **SGNSRV-Pool**.
12. Wählen Sie im **Aktionen** Bereich auf der linken Seite **Erweiterte Einstellungen**.
13. Klicken Sie in **Erweiterte Einstellungen** unter **Prozessmodell** für die Eigenschaft **Identität** auf die **...** Schaltfläche.
14. Wählen Sie in **Identität des Anwendungspools** die Option **Benutzerdefiniertes Konto** und klicken Sie auf **Festlegen**.
15. Geben Sie in **Anmeldeinformationen festlegen** den relevanten Windows-Benutzernamen in folgender Form ein: `Domäne\<Windows-Benutzername>`. Geben Sie das entsprechende Windows-Kennwort ein, bestätigen Sie es und klicken Sie auf **OK**.
16. Wählen Sie im Bereich **Verbindungen** auf der linken Seite den relevanten Server-Knoten und klicken Sie im **Aktionen** Bereich auf **Neu starten.**
17. Wählen Sie im Bereich **Verbindungen** auf der linken Seite unter dem relevanten Server-Knoten unter **Sites** , **Standard-Websites** die Option **SGNSRV**.
18. Doppelklicken Sie auf der /SGNSRV Homepage in der Mitte auf **Authentifizierung**.
19. Klicken Sie mit der rechten Maustaste auf **Anonyme Authentifizierung** und wählen Sie **Bearbeiten**.
20. Wählen Sie bei **Identität des anonymen Benutzers** die Option **Bestimmter Benutzer** und überprüfen Sie, ob der Benutzername **IUSR** lautet. Korrigieren Sie ihn, wenn nötig.
21. Klicken Sie auf **OK**.

Die zusätzliche Konfiguration für die Benutzung eines Windows-Kontos für die Anmeldung am SQL Server ist nun abgeschlossen.

5 Einrichten des SafeGuard Management Centers

Dieser Abschnitt beschreibt die Installation und Konfiguration des SafeGuard Management Center.

Das SafeGuard Management Center ist das zentrale Verwaltungswerkzeug für SafeGuard Enterprise. Installieren Sie es auf den Administrator-Computern, die Sie für die Verwaltung von SafeGuard Enterprise einsetzen möchten. Das SafeGuard Management Center kann auf jedem Rechner im Netzwerk installiert sein, von wo aus auf die SafeGuard Enterprise Datenbanken zugegriffen werden kann.

Mit datenbankspezifischen Konfigurationen (Multi Tenancy) ermöglicht das SafeGuard Management Center den Einsatz von SafeGuard Enterprise mit mehreren Datenbanken. Sie können verschiedene SafeGuard Enterprise Datenbanken für unterschiedliche Bereiche (z. B. Unternehmensstandorte, Organisationseinheiten oder Domänen) einrichten und verwalten. Um den Verwaltungsaufwand zu reduzieren, können Sie Datenbankkonfigurationen auch in Dateien exportieren und aus Dateien importieren.

Das SafeGuard Management Center muss nicht notwendigerweise nur auf einem Computer installiert sein. Es kann auf jedem Rechner im Netzwerk installiert sein, von wo aus auf die Datenbank zugegriffen werden kann.

5.1 Voraussetzungen

Folgende Voraussetzungen müssen erfüllt sein:

- Stellen Sie sicher, dass Sie über Windows Administratorrechte verfügen.
- .NET Framework 4 muss installiert sein. Das Programm steht in der SafeGuard Enterprise Produktlieferung zur Verfügung.
- Wenn Sie eine neue SafeGuard Enterprise Datenbank während der SafeGuard Management Center Konfiguration erzeugen wollen, benötigen Sie entsprechende SQL-Zugriffsberechtigungen, siehe *Datenbankzugriffsrechte* (Seite 17).
- Wenn die SafeGuard Enterprise Datenbank und das SafeGuard Management Center auf verschiedenen Computern installiert werden, gehen Sie sicher, dass der systemeigene SQL Server 2012 Client und die SQL Server 2012 Kommandozeilen-Tools auf dem Computer installiert werden, auf dem Sie das SafeGuard Management Center installiert haben. Diese sind im Drittanbieter-Ordner der SafeGuard Enterprise Produktlieferung enthalten.

5.2 Installieren des SafeGuard Management Center

1. Starten Sie SGNManagementCenter.msi aus dem Installationsordner Ihrer Produktlieferung. Ein Assistent führt Sie durch die notwendigen Schritte.

2. Übernehmen Sie die Standardeinstellungen in den nächsten Dialogen wie folgt. Führen Sie auf der **Installationsart auswählen** Seite einen der folgenden Schritte aus:
   - Wenn das SafeGuard Management Center nur eine Datenbank unterstützen soll, wählen Sie eine Installation vom Typ **Typisch** aus.
   - Wenn das SafeGuard Management Center mehrere Datenbanken unterstützen soll (**Multi Tenancy**), wählen Sie eine Installation vom Typ **Vollständig** aus. Für weitere Informationen, siehe *Multi Tenancy Konfigurationen* (Seite 27).

Das SafeGuard Management Center ist installiert. Starten Sie Ihren ggf. Computer neu. Im nächsten Schritt führen Sie die Erstkonfiguration im SafeGuard Management Center durch.

5.3 Anzeigen des SafeGuard Management Center Hilfesystems

Das SafeGuard Management Center Hilfesystem wird in Ihrem Browser angezeigt. Es bietet umfassende Features wie kontextsensitive Hilfe und Volltextsuche. Das Hilfesystem ist für die volle Funktionalität der Inhaltsseiten konfiguriert und aktiviert JavaScript in Ihrem Browser.

Beim Microsoft Internet Explorer zeigt sich folgendes Verhalten:

- Windows 7 - Internet Explorer 8 - Standardsicherheit:

  Es wird keine Sicherheitsleiste angezeigt, die angibt, dass der Internet Explorer die Scripting-Ausführung gesperrt hat.
  JavaScript wird ausgeführt.

Hinweis: Auch wenn JavaScript deaktiviert ist, können Sie das SafeGuard Management Center Hilfesystem aufrufen und im System navigieren. Bestimmte Funktionen, z. B. Suchen, lassen sich dann jedoch nicht anzeigen.

5.4 Konfigurieren des SafeGuard Management Center

Nach der Installation müssen Sie das SafeGuard Management Center konfigurieren. Der SafeGuard Management Center Konfigurationsassistent unterstützt Sie bei der Erstkonfiguration durch Hilfestellung bei der Definition der grundlegenden SafeGuard Management Center Einstellungen sowie bei der Konfiguration der Datenbankverbindung. Der Assistent wird automatisch aufgerufen, wenn Sie das SafeGuard Management Center zum ersten Mal nach der Installation starten.

Sie können das SafeGuard Management Center für die Anwendung mit einer oder mehreren Datenbank (Multi Tenancy) konfigurieren.

Hinweis: Die folgenden Schritte müssen mit dem Konfigurationsassistenten sowohl für Single Tenancy als auch für Multi Tenancy Konfigurationen ausgeführt werden.

5.4.1 Voraussetzungen

Folgende Voraussetzungen müssen erfüllt sein:

- Stellen Sie sicher, dass Sie über Windows Administratorrechte verfügen.

- Halten Sie die folgenden Informationen bereit. Diese erhalten Sie ggf. von Ihrem SQL-Administrator.

  SQL Anmeldeinformationen
  Name des SQL Servers, auf dem die SafeGuard Enterprise Datenbank laufen soll.
  Name der SafeGuard Enterprise Datenbank, falls diese bereits erzeugt wurde.

5.4.2 Multi Tenancy Konfigurationen

Sie können mehrere verschiedene SafeGuard Enterprise Datenbankkonfigurationen für eine Instanz des SafeGuard Management Center konfigurieren und verwalten. Dies erweist sich vor allem dann als nützlich, wenn Sie verschiedene Konfigurationen für verschiedene Domänen, Organisationseinheiten oder Unternehmensstandorte einsetzen möchten.

Hinweis: Sie müssen pro Datenbank (Mandant) jeweils eine separate SafeGuard Enterprise Server Instanz einrichten.

Zur Vereinfachung der Konfiguration können neu erstellte Datenbankkonfigurationen zur späteren Wiederverwendung in eine Datei exportiert werden und zuvor erstellte Konfigurationen aus einer Datei eingelesen werden.

Um das SafeGuard Management Center für Multi Tenancy zu konfigurieren, führen Sie zunächst die initiale Konfiguration und danach weitere spezifische Schritte für die Multi Tenancy Konfiguration durch.

5.4.3 Starten der Erstkonfiguration des SafeGuard Management Centers

Nach der Installation des SafeGuard Management Center, müssen Sie die Erstkonfiguration durchführen. Die Erstkonfiguration muss sowohl für den Single Tenancy als auch für den Multi Tenancy Modus ausgeführt werden.

So starten Sie den SafeGuard Management Center Konfigurationsassistenten:

1. Starten Sie das **SafeGuard Management Center** über das **Start** Menü. Der Konfigurationsassistent wird gestartet und führt Sie durch die notwendigen Schritte.
2. Klicken Sie auf der **Willkommen** Seite auf **Weiter**.

5.4.4 Konfigurieren der Datenbankserver-Verbindung

Zum Speichern aller SafeGuard Enterprise spezifischen Verschlüsselungsrichtlinien und Einstellungen wird eine Datenbank verwendet. Damit das SafeGuard Management Center mit dem SafeGuard Enterprise Server kommunizieren kann, müssen Sie eine Authentisierungsmethode für den Zugriff auf die Datenbank festlegen, entweder Windows NT Authentisierung oder SQL-Authentisierung. Wenn Sie eine Verbindung zum Datenbankserver mit SQL Authentisierung herstellen möchten, stellen Sie sicher, dass Sie die

notwendigen SQL-Anmeldedaten zur Hand haben. Falls notwendig, erhalten Sie diese Informationen von Ihrem SQL Administrator.

1. Führen Sie auf der Seite **Datenbankserver-Verbindung** folgende Schritte aus:
   - Wählen Sie unter **Verbindungseinstellungen** den SQL-Datenbankserver aus der **Datenbankserver** Liste aus. Es werden alle Rechner eines Netzwerks aufgelistet, auf denen ein Microsoft SQL Server installiert ist. Wenn der Server nicht auswählbar ist, tragen Sie Servername bzw. IP-Adresse mit dem SQL-Instanznamen manuell ein.
   - Aktivieren Sie **SSL verwenden**, um die Verbindung zwischen SafeGuard Management Center und SQL-Datenbankserver zu sichern. Wenn Sie **Folgende Anmeldeinformationen für SQL Server Authentisierung anwenden** unter **Authentisierung** auswählen, empfehlen wir dringend, diese Einstellung zu aktivieren, da dadurch der Transport der SQL-Anmeldedaten verschlüsselt wird. SSL-Verschlüsselung erfordert eine funktionsfähige SSL-Umgebung auf dem SQL Datenbankserver, die Sie vorab einrichten müssen, siehe *Sichern von Transportverbindungen mit SSL* (Seite 40).

2. Wählen Sie unter **Authentisierung** die Art der Authentisierung, die für den Zugriff auf die Datenbankserverinstanz benutzt werden soll. Dies ist erforderlich, damit das SafeGuard Management Center mit der Datenbank kommunizieren kann:
   - Aktivieren Sie **Windows NT Authentisierung verwenden**, um Ihre Windows-Anmeldedaten zu verwenden.

     Hinweis: Verwenden Sie diese Art der Authentisierung, wenn Ihr Computer Teil einer Domäne ist. In diesem Fall sind jedoch zusätzliche Konfigurationsschritte notwendig, da der Benutzer dazu berechtigt sein muss, eine Verbindung mit der Datenbank herzustellen, siehe *Konfigurieren eines Windows-Benutzerkontos für die Anmeldung am SQL Server* (Seite 18) und *Konfigurieren der Windows-Authentisierung für die Anmeldung am SQL Server* (Seite 23).
   - Aktivieren Sie **Folgende Anmeldeinformationen für SQL Server Authentisierung anwenden**, um mit den entsprechenden SQL-Anmeldeinformationen auf die Datenbank zuzugreifen. Geben Sie die Anmeldeinformationen des SQL-Benutzerkontos ein, das Ihr SQL-Administrator erstellt hat. Falls notwendig, erhalten Sie diese Informationen von Ihrem SQL Administrator.

     Hinweis: Verwenden Sie diese Art der Authentisierung, wenn Ihr Computer keiner Domäne angehört. Aktivieren Sie **SSL verwenden**, um die Verbindung zum und vom Datenbankserver zu sichern.

3. Klicken Sie auf **Weiter**.

Die Verbindung zum Datenbankserver ist hergestellt.

5.4.5 Erstellen oder Auswählen einer Datenbank

Legen Sie auf der Seite **Datenbankeinstellungen** fest, ob eine existierende Datenbank oder eine neue Datenbank zum Speichern der Administrationsdaten benutzt werden soll.

1. Gehen Sie wie folgt vor:

   - Wenn noch keine Datenbank existiert, wählen Sie **Eine neue Datenbank mit folgendem Namen erstellen**. Geben Sie einen Namen für die neue Datenbank ein. Sie benötigen dazu die entsprechenden SQL-Zugriffsberechtigungen, siehe *Datenbankzugriffsrechte* (Seite 17). Um Probleme zu vermeiden, sollten in SafeGuard Enterprise Datenbanknamen nur folgende Zeichen verwendet werden: Buchstaben (A - Z, a - z), Zahlen (0 - 9), Unterstriche (_).
   - Wenn bereits eine Datenbank angelegt wurde oder wenn Sie das SafeGuard Management Center bereits auf einem anderen Computer installiert haben, klicken Sie auf **Folgende bestehende Datenbank wählen** und wählen Sie die entsprechende Datenbank aus der Liste aus.

2. Klicken Sie auf **Weiter**.

5.4.6 Erstellen eines Haupt-Sicherheitsbeauftragten (Master Security Officer, MSO)

Als Sicherheitsbeauftragter melden Sie sich am SafeGuard Management Center an, um SafeGuard Enterprise Richtlinien zu erstellen und die Verschlüsselungssoftware für die Endbenutzer zu konfigurieren.

Der Haupt-Sicherheitsbeauftragte (MSO) ist der Administrator höchster Ebene mit allen Rechten und einem Zertifikat, das nicht abläuft.

1. Geben Sie auf der Seite **Daten des Sicherheitsbeauftragten** unter **Haupt-Sicherheitsbeauftragten-ID** einen Namen für den Haupt-Sicherheitsbeauftragten ein.
2. Geben Sie unter **Anmeldung mit Token** an, ob Sie einen Token/eine Smartcard für die Anmeldung benutzen möchten oder nicht.

   Wir empfehlen, dass Sie die Anmeldung mit Token nicht als **Zwingend erforderlich** definieren. Eine Anmeldung mit Token bzw. Smartcard erfordert eine gesonderte Konfiguration, die innerhalb des SafeGuard Management Centers zu erledigen ist.
3. Führen Sie auf der Seite **Zertifikat für den Haupt-Sicherheitsbeauftragten** einen der folgenden Schritte aus:

   - Klicken Sie auf **Erzeugen**, um ein neues Zertifikat für den Haupt-Sicherheitsbeauftragten zu erzeugen. Sie werden dazu aufgefordert, sowohl für den Zertifikatsspeicher als auch für die Datei, in die das Zertifikat exportiert werden soll (private Schlüsseldatei P12), jeweils ein Kennwort einzugeben und zu bestätigen. Das Zertifikat wird erzeugt und unter **Zertifikat für den Haupt-Sicherheitsbeauftragten** angezeigt.

- Klicken Sie auf **Importieren**, um ein Zertifikat für den Haupt-Sicherheitsbeauftragten zu verwenden, das bereits auf dem Netz zur Verfügung steht. Suchen Sie unter **Importieren des Zertifikats** die gesicherte Schlüsseldatei. Geben Sie unter **Kennwort der Datei** das für diese Datei festgelegte Kennwort ein und bestätigen Sie es. Wählen Sie **Schlüsseldatei im Zertifikatsspeicher speichern** und geben Sie das Kennwort für den Speicher ein. Klicken Sie auf **OK**. Das Zertifikat wird importiert und unter **Zertifikat für den Haupt-Sicherheitsbeauftragten** angezeigt.

Der Haupt-Sicherheitsbeauftragte benötigt das Kennwort des Zertifikatsspeichers für die Anmeldung am SafeGuard Management Center. Notieren Sie sich das Kennwort und bewahren Sie es an einem sicheren Ort auf. Steht das Kennwort nicht mehr zur Verfügung, so kann sich der Haupt-Sicherheitsbeauftragte nicht mehr am SafeGuard Management Center anmelden.

Für die Wiederherstellung einer beschädigten SafeGuard Management Center Installation benötigt der Haupt-Sicherheitsbeauftragte die private Schlüsseldatei.

4. Klicken Sie auf **Weiter**.

Der Haupt-Sicherheitsbeauftragte wird angelegt.

5.4.6.1 Erzeugen des Zertifikats des Haupt-Sicherheitsbeauftragten

Gehen Sie in **Zertifikat des Haupt-Sicherheitsbeauftragten erzeugen** folgendermaßen vor:

1. Bestätigen Sie unter **Haupt-Sicherheitsbeauftragten-ID** den Namen des Haupt-Sicherheitsbeauftragten.
2. Geben Sie nun zweimal das Kennwort für den Zertifikatsspeicher ein und klicken Sie auf **OK**.

Das Zertifikat des Haupt-Sicherheitsbeauftragten wird erzeugt und lokal als Backup (<mso_name>.cer) gespeichert.

Hinweis: Notieren Sie sich das Kennwort und bewahren Sie es an einem sicheren Ort auf. Sie müssen sich am SafeGuard Management Center anmelden.

5.4.6.2 Export des Zertifikats des Haupt-Sicherheitsbeauftragten

Das Zertifikat des Haupt-Sicherheitsbeauftragten wird in eine Datei exportiert, die so genannte private Schlüsseldatei (P12). Diese ist mit einem Kennwort gesichert. Das Zertifikat des Haupt-Sicherheitsbeauftragten ist dadurch zusätzlich geschützt. Die private Schlüsseldatei wird für die Wiederherstellung einer beschädigten SafeGuard Management Center Installation benötigt.

So exportieren Sie das Zertifikat eines Haupt-Sicherheitsbeauftragten:

1. Geben Sie unter **Zertifikat exportieren** ein Kennwort für den privaten Schlüssel (P12-Datei) ein und bestätigen Sie es. Das Kennwort muss aus 8 alphanumerischen Zeichen bestehen.
2. Klicken Sie auf **OK**.
3. Geben Sie einen Speicherort für die private Schlüsseldatei ein.

Die private Schlüsseldatei wird erzeugt und die Datei wird am angegebenen Speicherort gespeichert <mso_name.p12).

Hinweis: Erstellen Sie eine Sicherungskopie des privaten Schlüssels (P12-Datei) und legen Sie diese direkt nach der Erstkonfiguration an einem sicheren Speicherort ab. Andernfalls führt ein eventueller PC-Absturz zum Verlust des Schlüssels und SafeGuard Enterprise muss neu installiert werden. Das gilt für alle von SafeGuard Enterprise generierten Sicherheitsbeauftragten-Zertifikate. Weitere Informationen finden Sie in der *SafeGuard Enterprise Administratorhilfe* im Kapitel *Unternehmenszertifikat und Master Security Officer Zertifikat exportieren*.

5.4.6.3 Import des Zertifikats des Haupt-Sicherheitsbeauftragten

Wenn bereits ein Zertifikat eines Haupt-Sicherheitsbeauftragten zur Verfügung steht, müssen Sie es in den Zertifikatsspeicher importieren.

Hinweis: Ein Zertifikat kann nicht aus einer Microsoft PKI importiert werden. Ein importiertes Zertifikat muss minimal 1024 Bits haben und kann maximal 4096 Bits lang sein.

1. Klicken Sie unter **Authentisierungs-Schlüsseldatei importieren** auf die [**...**] Schaltfläche und wählen Sie die Schlüsseldatei aus. Geben Sie das **Kennwort der Schlüsseldatei** ein. Geben Sie das zuvor unter **Kennwort des Zertifikatsspeichers oder Token-PIN** definierte Kennwort für den Zertifikatsspeicher ein. Wählen Sie **In den Zertifikatsspeicher importieren** oder **Auf den Token kopieren**, um das Zertifikat auf einem Token zu speichern.
2. Geben Sie zur Initialisierung des Zertifikatsspeichers das Kennwort noch einmal ein.

Zertifikat und privater Schlüssel befinden sich nun im Zertifikatsspeicher. Zur Anmeldung an das SafeGuard Management Center wird das Kennwort des Zertifikatsspeichers verwendet.

5.4.7 Erzeugen des Unternehmenszertifikats

Mit dem Unternehmenszertifikat lassen sich unterschiedliche SafeGuard Management Center Installationen auseinander halten. In Verbindung mit dem Zertifikat des Haupt-Sicherheitsbeauftragten lässt sich mit dem Unternehmenszertifikat eine beschädigte SafeGuard Enterprise Datenbankkonfiguration wiederherstellen.

1. Wählen Sie auf der Seite **Unternehmenszertifikat** die Option **Neues Unternehmenszertifikat erzeugen**.
2. Geben Sie einen Namen Ihrer Wahl ein.

   Hinweis: Von SafeGuard Enterprise erzeugte Zertifikate, zum Beispiel Unternehmens-, Maschinen-, Sicherheitsbeauftragten- und Benutzerzertifikate, sind bei einer Erstinstallation standardmäßig zur Erweiterung der Sicherheit mit dem Hash-Algorithmus **SHA-256** signiert.

   Wenn Sie noch SafeGuard Enterprise Endpoints mit Version 6 oder einer früheren Version mit dem SafeGuard Management Center der Version 6.1 verwalten müssen, müssen Sie unter **Hash-Algorithmus für erzeugte Zertifikate** den Algorithmus **SHA-1** auswählen. Weitere Informationen finden Sie in der SafeGuard Enterprise Administrator Hilfe im Abschnitt *Ändern des Algorithmus für selbst-signierte Zertifikate*.

   Der ausgewählte Algorithmus wird zum Signieren aller von SafeGuard Enterprise erzeugten Zertifikate benutzt. Dies sind die Unternehmens- und Maschinenzertifikate sowie die Sicherheitsbeauftragten- und Benutzerzertifikate.

3. Klicken Sie auf **Weiter**.

Das neu angelegte Unternehmenszertifikat wird in der Datenbank gespeichert.

Erstellen Sie eine Sicherungskopie des Unternehmenszertifikats und legen Sie diese direkt nach der Erstkonfiguration an einem sicheren Speicherort ab.

Für Informationen zum Wiederherstellen einer beschädigten Datenbankkonfiguration, siehe *Wiederherstellen einer beschädigten Datenbankkonfiguration* (Seite 36).

5.4.8 Abschließen der Erstkonfiguration des SafeGuard Management Centers

1. Klicken Sie auf **Beenden**, um die Erstkonfiguration des SafeGuard Management Centers abzuschließen.

Eine Konfigurationsdatei wird erstellt.

Ergebnis:

- Eine Verbindung zum SafeGuard Enterprise Server.
- Eine SafeGuard Enterprise Datenbank.
- Ein Haupt-Sicherheitsbeauftragten-Konto für die Anmeldung an das SafeGuard Management Center
- Alle notwendigen Zertifikate für die Wiederherstellung einer beschädigten Datenbankkonfiguration oder SafeGuard Management Center Installation

Sobald der Konfigurationsassistent geschlossen ist, wird das SafeGuard Management Center gestartet.

5.5 Erstellen weiterer Datenbankkonfigurationen (Multi Tenancy)

Voraussetzung: Die Funktion Multi Tenancy muss über eine Installation vom Typ **Vollständig** installiert worden sein. Die initiale Konfiguration des SafeGuard Management Center muss durchgeführt worden sein, siehe *Starten der Erstkonfiguration des SafeGuard Management Centers* (Seite 27).

Hinweis: Sie müssen pro Datenbank jeweils eine separate SafeGuard Enterprise Server Instanz einrichten.

So erstellen Sie eine weitere SafeGuard Enterprise Datenbankkonfiguration nach der Erstkonfiguration:

1. Starten Sie das SafeGuard Management Center. Der Dialog **Konfiguration auswählen** wird angezeigt.
2. Klicken Sie auf **Neu**. Der SafeGuard Management Center Konfigurationsassistent wird automatisch gestartet.
3. Der Assistent führt Sie durch die notwendigen Schritte für das Anlegen einer neuen Datenbankkonfiguration. Nehmen Sie die erforderlichen Einstellungen vor. Die neue Datenbankkonfiguration wird generiert.

4. Zur Authentisierung werden Sie dazu aufgefordert, den Sicherheitsbeauftragtennamen für diese Konfiguration auszuwählen und das entsprechende Zertifikatsspeicherkennwort einzugeben. Klicken Sie auf **OK**.

Das SafeGuard Management Center wird geöffnet und mit der ausgewählten Datenbankkonfiguration verbunden. Wenn Sie das SafeGuard Management Center das nächste Mal starten, können Sie die neue Datenbank-Konfiguration aus der Liste auswählen.

Hinweis: Weitere Informationen zu Multi Tenancy finden Sie in der *SafeGuard Enterprise Administratorhilfe* im Kapitel *Mit mehreren Datenbankkonfigurationen arbeiten*.

5.6 Konfigurieren zusätzlicher Instanzen des SafeGuard Management Center

Sie können zusätzliche Instanzen des SafeGuard Management Center konfigurieren, um Sicherheitsbeauftragten den Zugriff für die Durchführung administrativer Aufgaben auf verschiedenen Computern zu ermöglichen. Das SafeGuard Management Center kann auf jedem Rechner im Netzwerk installiert sein, von wo aus auf die Datenbank zugegriffen werden kann.

SafeGuard Enterprise verwaltet die Zugriffsrechte auf das SafeGuard Management Center in einem eigenen Zertifikatsverzeichnis. In diesem Verzeichnis müssen die Zertifikate aller Sicherheitsbeauftragten, die sich am SafeGuard Management Center anmelden dürfen, vorhanden sein. Für die Anmeldung an das SafeGuard Management Center ist dann nur das Kennwort für den Zertifikatsspeicher erforderlich.

1. Installieren Sie SGNManagementCenter.msi mit den gewünschten Features auf einem weiteren Computer.
2. Starten Sie das SafeGuard Management Center auf dem Computer mit dem neu installierten SafeGuard Management Center. Der Konfigurationsassistent wird gestartet und führt Sie durch die notwendigen Schritte.
3. Klicken Sie auf der **Willkommen** Seite auf **Weiter**.
4. Wählen Sie im Dialog **Datenbankverbindung** unter **Datenbankserver** die erforderliche SQL-Datenbankinstanz aus der Liste aus. Alle auf Ihrem Computer oder Netzwerk verfügbaren Datenbankserver werden angezeigt. Wählen Sie unter **Authentisierung** die Art der Authentisierung, die für den Zugriff auf diese Datenbankinstanz benutzt werden soll. Wenn Sie **Folgende Anmeldeinformationen für SQL Server Authentisierung anwenden** wählen, geben Sie die SQL-Benutzerkontenanmeldedaten ein, die Ihr SQL-Administrator erstellt hat. Klicken Sie auf **Weiter**.
5. Aktivieren Sie unter **Datenbankeinstellungen** die Option **Folgende bestehende Datenbank verwenden** und wählen Sie die Datenbank aus der Liste aus. Klicken Sie auf **Weiter**.
6. Wählen Sie unter **SafeGuard Management Center Authentisierung** eine autorisierte Person aus der Liste aus. Wenn Multi Tenancy aktiviert ist, zeigt der Dialog an, an welcher Konfiguration sich der Benutzer anmeldet. Geben Sie das Kennwort für den Zertifikatsspeicher ein und bestätigen Sie es.

   Der Zertifikatsspeicher für das aktuelle Benutzerkonto wird angelegt und ist durch dieses abgesichert. Für die nachfolgenden Anmeldungen benötigen Sie nur noch dieses Kennwort.

7. Klicken Sie auf **OK**.

   Eine Meldung, dass Zertifikat und privater Schlüssel nicht gefunden bzw. nicht darauf zugegriffen werden kann, wird angezeigt.

8. Klicken Sie zum Importieren der Daten auf **Ja** und dann auf **OK**. Dadurch wird der Importvorgang gestartet.
9. Klicken Sie unter **Authentisierungs-Schlüsseldatei importieren** auf die [**...**] Schaltfläche und wählen Sie die Schlüsseldatei aus. Geben Sie das **Kennwort der Schlüsseldatei** ein. Geben Sie das zuvor unter **Kennwort des Zertifikatsspeichers oder Token-PIN** definierte Kennwort für den Zertifikatsspeicher ein. Wählen Sie **In den Zertifikatsspeicher importieren** oder **Auf den Token kopieren**, um das Zertifikat auf einem Token zu speichern.
10. Geben Sie zur Initialisierung des Zertifikatsspeichers das Kennwort noch einmal ein.

Zertifikat und privater Schlüssel befinden sich nun im Zertifikatsspeicher. Zur Anmeldung an das SafeGuard Management Center wird das Kennwort des Zertifikatsspeichers verwendet.

5.7 Anmeldung am SafeGuard Management Center

Die Anmeldung richtet sich danach, ob Sie das SafeGuard Management Center im Single Tenancy Modus oder im Multi Tenancy Modus einsetzen.

Informationen zu den ersten Arbeitsschritten im SafeGuard Management Center finden Sie in der *SafeGuard Enterprise Administratorhilfe*.

5.7.1 Anmeldung im Single Tenancy Modus

1. Starten Sie das SafeGuard Management Center über das **Start**-Menü. Ein Anmeldebildschirm wird angezeigt.
2. Melden Sie sich als Haupt-Sicherheitsbeauftragter an und geben Sie das Zertifikatsspeicherkennwort ein, das während der Konfiguration festgelegt wurde. Klicken Sie auf **OK**.

Das SafeGuard Management Center wird gestartet.

Hinweis: Wenn Sie ein falsches Kennwort eingeben, wird eine Fehlermeldung angezeigt und die nächste Anmeldung wird verzögert. Diese Verzögerung wird mit jedem fehlgeschlagenen Anmeldeversuch größer. Fehlgeschlagene Anmeldeversuche werden protokolliert.

5.7.2 Anmeldung im Multi Tenancy Modus

Wenn Sie mehrere Datenbanken konfiguriert haben (Multi Tenancy), erweitert sich der Anmeldevorgang am SafeGuard Management Center.

1. Starten Sie das SafeGuard Management Center über den Produktordner im **Start** Menü. Der Dialog **Konfiguration auswählen** wird angezeigt.
2. Wählen Sie die Datenbankkonfiguration aus, die Sie verwenden möchten, und klicken Sie auf **OK**. Die ausgewählte Datenbankkonfiguration wird mit dem SafeGuard Management Center verbunden und wird aktiv.

3. Sie werden dazu aufgefordert, den Sicherheitsbeauftragtennamen für diese Konfiguration auszuwählen und das entsprechende Zertifikatsspeicherkennwort einzugeben. Klicken Sie auf **OK**.

Das SafeGuard Management Center wird geöffnet und mit der ausgewählten Datenbankkonfiguration verbunden.

Hinweis: Wenn Sie ein falsches Kennwort eingeben, wird eine Fehlermeldung angezeigt und die nächste Anmeldung wird verzögert. Diese Verzögerung wird mit jedem fehlgeschlagenen Anmeldeversuch größer. Fehlgeschlagene Anmeldeversuche werden protokolliert.

5.8 Einrichten der Organisationsstruktur im SafeGuard Management Center

Es gibt zwei Möglichkeiten, Ihre Organisation in SafeGuard Enterprise abzubilden:

- Directory Service importieren, z. B.: Active Directory

  Während der Synchronisierung mit dem Active Directory werden Objekte (z. B. Computer, Benutzer und Gruppen) in das SafeGuard Management Center importiert und in der SafeGuard Enterprise Datenbank gespeichert.

- Organisationsstruktur manuell aufbauen

  Steht kein Directory Service zur Verfügung oder gibt es nur wenige Organisationseinheiten, so dass kein Directory Service benötigt wird, können Sie neue Domänen/Arbeitsgruppen anlegen, an denen sich der Benutzer/Computer anmelden kann.

Sie können entweder nur eine von beiden Möglichkeiten anwenden, oder die beiden Möglichkeiten mischen. Zum Beispiel können Sie ein Active Directory (AD) ganz oder teilweise importieren und weitere Organisationseinheiten (OU) manuell anlegen. Egal, ob die Organisationsstruktur importiert oder manuell angelegt wird, die Richtlinienzuordnung kann in beiden Fällen erfolgen.

Hinweis: Bei der Kombination beider Verfahren werden die manuell angelegten Organisationseinheiten nicht im AD abgebildet. Wenn in SafeGuard Enterprise angelegte Organisationseinheiten im AD abgebildet werden sollen, so müssen Sie diese separat zum AD hinzufügen.

Weitere Informationen zum Importieren oder Anlegen einer Organisationsstruktur finden Sie in der *SafeGuard Enterprise Administratorhilfe* im Kapitel *Aufbau der Organisationsstruktur*.

5.9 Importieren der Lizenzdatei

SafeGuard Enterprise hat einen integrierten Lizenzzähler. Die Installation umfasst standardmäßig für jede SafeGuard Enterprise Komponente eine festgelegte Anzahl von 5 Lizenzen. Dadurch soll eine problemlose Evaluierung von anderen SafeGuard Enterprise Komponenten ohne Nebeneffekte gewährleistet werden. Beim Kauf von SafeGuard Enterprise enthält jeder Kunde eine individuelle Lizenzdatei für das jeweilige Unternehmen, die in das SafeGuard Management Center importiert werden muss.

Detaillierte Informationen hierzu finden Sie im Kapitel *Lizenzen* der *SafeGuard Enterprise Administrator-Hilfe*.

5.10 Wiederherstellen einer beschädigten SafeGuard Enterprise Installation

Wenn eine SafeGuard Management Center Installation beschädigt, jedoch die Datenbank noch intakt ist, kann die Installation auf einfache Art und Weise wiederhergestellt werden. In diesem Fall müssen Sie nur das SafeGuard Management Center neu installieren und die vorhandene Datenbank sowie das gesicherte Haupt-Sicherheitsbeauftragten-Zertifikat verwenden.

- Das Unternehmenszertifikat und das Haupt-Sicherheitsbeauftragten-Zertifikat der betreffenden Datenbankkonfiguration müssen als .p12 Dateien exportiert worden sein. Die Dateien müssen vorhanden und gültig sein.
- Die Kennwörter für die beiden .p12 Dateien und für den Zertifikatsspeicher müssen Ihnen bekannt sein.

So stellen Sie eine beschädigte SafeGuard Management Center Installation wieder her:

1. Installieren Sie das SafeGuard Management Center Installationspaket neu. Öffnen Sie das SafeGuard Management Center. Der Konfigurationsassistent wird automatisch geöffnet.
2. Wählen Sie auf der Seite **Datenbankverbindung** den relevanten Datenbankserver und konfigurieren Sie, falls erforderlich, die Verbindung zur Datenbank. Klicken Sie auf **Weiter**.
3. Aktivieren Sie auf der Seite **Datenbankeinstellungen** die Option **Folgende bestehende Datenbank verwenden** und wählen Sie die Datenbank aus der Liste aus.
4. Führen Sie auf der Seite **Daten des Sicherheitsbeauftragten** Seite einen der folgenden Schritte aus:
   - Wenn die gesicherte Zertifikatsdatei auf dem Computer gefunden wird, wird sie angezeigt. Geben Sie das Kennwort ein, das Sie zur Anmeldung an das SafeGuard Management Center benutzen.
   - Wird die gesicherte Zertifikatsdatei nicht auf dem Computer gefunden, wählen Sie **Importieren**. Suchen Sie nach der gesicherten Zertifikatsdatei und klicken Sie auf **Öffnen**. Geben Sie das Kennwort für die Zertifikatsdatei ein. Klicken Sie auf **Ja**. Geben Sie ein Kennwort für die Anmeldung am SafeGuard Management Center ein und bestätigen Sie es.
5. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**, um die Konfiguration des SafeGuard Management Center abzuschließen.

Die SafeGuard Management Center Installation ist wiederhergestellt.

5.11 Wiederherstellen einer beschädigten Datenbankkonfiguration

Sie können eine beschädigte Datenbankkonfiguration wiederherstellen, indem Sie das SafeGuard Management Center neu installieren und basierend auf den gesicherten Zertifikatsdateien

eine neue Instanz der Datenbank erstellen. Dadurch wird sichergestellt, dass alle vorhandenen SafeGuard Enterprise Endpoints Richtlinien von der neuen Installation annehmen.

- Das Unternehmenszertifikat und das Haupt-Sicherheitsbeauftragten-Zertifikat der betreffenden Datenbankkonfiguration müssen als .p12 Dateien exportiert worden sein. Die Dateien müssen vorhanden und gültig sein. Erstellen Sie Zertifikate-Backups im SafeGuard Management Center.

- Die Kennwörter für die beiden .p12 Dateien sowie für den Zertifikatsspeicher müssen Ihnen bekannt sein.

Hinweis: Diese Art der Wiederherstellung ist nur dann zu empfehlen, wenn keine gültige Sicherungskopie der Datenbank verfügbar ist. Alle Computer, die eine Verbindung mit einem auf diese Weise wiederhergestellten Backend herstellen, verlieren ihre Benutzer-Computer-Zuordnung. Dies hat zur Folge, dass die Power-on Authentication vorübergehend ausgeschaltet ist. Challenge/Response-Mechanismen stehen erst dann wieder zur Verfügung, wenn der entsprechende Endpoint seine Schlüsselinformationen wieder erfolgreich übertragen hat.

So stellen Sie eine beschädigte Datenbank wieder her:

1. Installieren Sie das SafeGuard Management Center Installationspaket neu. Öffnen Sie das SafeGuard Management Center. Der Konfigurationsassistent wird automatisch geöffnet.
2. Wählen Sie auf der **Datenbankverbindung** Seite die Option **Neue Datenbank erstellen**. Konfigurieren Sie unter **Datenbankeinstellungen** die Verbindung zur Datenbank. Klicken Sie auf **Weiter**.
3. Wählen Sie auf der Seite **Daten des Sicherheitsbeauftragten** den relevanten Haupt-Sicherheitsbeauftragten und klicken Sie auf **Importieren**.
4. Suchen Sie unter **Importieren des Zertifikats** die gesicherte Schlüsseldatei. Geben Sie unter **Kennwort der Datei** das für diese Datei festgelegte Kennwort ein und bestätigen Sie es. Wählen Sie **Schlüsseldatei im Zertifikatsspeicher speichern** und geben Sie das Kennwort für den Speicher ein. Klicken Sie auf **OK**.
5. Das Zertifikat des Haupt-Sicherheitsbeauftragten wird importiert. Klicken Sie auf **Weiter**.
6. Aktivieren Sie auf der Seite **Unternehmenszertifikat** die Option **Über vorhandenes Unternehmenszertifikat wiederherstellen**. Klicken Sie auf **Importieren**, um die gesicherte Zertifikatsdatei auszuwählen, die das gültige Unternehmenszertifikat enthält. Sie werden aufgefordert, das für den Zertifikatsspeicher definierte Kennwort einzugeben. Geben Sie das Kennwort ein und klicken Sie auf **OK**. Bestätigen Sie die angezeigte Meldung mit **Ja**. Das Unternehmenszertifikat wird importiert.
7. Klicken Sie auf **Weiter**, dann auf **Beenden**.

Die Datenbankkonfiguration ist wiederhergestellt.

6 Testen der Kommunikation

Wenn SafeGuard Enterprise Server, die Datenbank und das SafeGuard Management Center eingerichtet sind, sollten Sie einen Verbindungstest durchführen. Dieser Abschnitt beschreibt die erforderlichen Schritte.

6.1 Voraussetzungen

Vor dem Verbindungstest müssen folgende Einstellungen gemacht bzw. geprüft werden:

6.1.1 Ports/Verbindungen

Die Endpoints müssen folgende Verbindungen aufbauen:

SafeGuard Endpoint Verbindung zu	Port
SafeGuard Enterprise Server	Port 80/TCP Port 443 bei Benutzung der SSL Transportverbindung

Das SafeGuard Management Center muss folgende Verbindungen aufbauen:

SafeGuard Management Center Verbindung zu	Port
SQL Datenbank	SQL Server 2008 dynamischer Port: Port 1433/TCP und Port 1434/TCP
Active Directory	Port 389/TCP
SLDAP	Port 636 für den Active Directory Import

Der SafeGuard Enterprise Server muss folgende Verbindungen aufbauen:

SafeGuard Enterprise Server Verbindung zu	Port
SQL Datenbank	Port 1433/TCP und Port 1434/TCP für SQL 2008 (Express) dynamischer Port
Active Directory	Port 389/TCP

6.1.2 Authentisierungsmethode

1. Öffnen Sie auf dem Computer, auf dem SafeGuard Enterprise Server installiert ist, den **Internet Information Services (IIS) Manager**.
2. Klicken Sie in der Baumstruktur auf **Internet Information Services Manager**. Klicken Sie auf **Servername**, **Websites**, **Standard-Website**.
3. Klicken Sie mit der rechten Maustaste auf **SGNSRV** und klicken Sie auf **Eigenschaften**.
4. Klicken Sie auf die Registerkarte **Verzeichnissicherheit**.
5. Klicken Sie unter **Authentifizierung und Zugriffssteuerung** auf **Bearbeiten**. In **Authentifizierungsverfahren** wählen Sie **Anonymen Zugriff aktivieren**. Deaktivieren Sie unter **Authentifizierter Zugriff** das Kontrollkästchen **Integrierte Windows-Authentifizierung**.

6.1.3 Proxyserver-Einstellungen für Webserver und Endpoint

Definieren Sie die Proxyserver-Einstellungen wie folgt:

1. Klicken Sie im Internet Explorer im **Extras** Menü auf **Internetoptionen**. Klicken Sie auf **Verbindungen** und dann auf **LAN-Einstellungen**.
2. Deaktivieren Sie in **LAN-Einstellungen** unter **Proxyserver** das Kontrollkästchen **Proxyserver für LAN verwenden**.

   Wenn ein Proxyserver notwendig ist, wählen Sie **Proxyserver für lokale Adressen umgehen**.

6.2 Testen der Verbindung (IIS 7 auf Windows Server 2008)

1. Öffnen Sie auf dem Computer, auf dem SafeGuard Enterprise Server installiert ist, den **Internet Information Services (IIS) Manager**.
2. Klicken Sie in der Baumstruktur auf **"Servername"**, **Seiten**, **Standard-Web-Seite**. Überprüfen Sie, ob die Web-Seite **SGNSRV** im Ordner **Standard-Web-Seite** verfügbar ist.
3. Klicken Sie mit der rechten Maustaste auf **SGNSRV**, wählen Sie **Anwendung verwalten** und klicken Sie auf **Browse**, um die **SGNSRV Home** Seite **Sophos SafeGuard Web Service** zu öffnen.
4. Auf der Seite **Sophos SafeGuard Web Service** wird eine Liste mit möglichen Aktionen angezeigt. Klicken Sie in dieser Liste auf **CheckConnection**.
5. Klicken Sie auf der **CheckConnection** Seite auf **Aufrufen**.

Der Verbindungstest war erfolgreich, wenn Sie diese Ausgabe erhalten:



7 Sichern von Transportverbindungen mit SSL

SafeGuard Enterprise unterstützt zur Erhöhung der Sicherheit die Verschlüsselung der Transportverbindungen zwischen den einzelnen Komponenten mit SSL.

- Die Verbindung zwischen dem Datenbankserver und dem Web Server sowie die Verbindung zwischen dem Datenbankserver und dem Computer, auf dem das SafeGuard Management Center installiert ist, kann mit SSL verschlüsselt werden.
- Die Verbindung zwischen dem SafeGuard Enterprise Server und dem von SafeGuard Enterprise verwalteten Computer kann entweder mit SSL oder mit SafeGuard-spezifischer Verschlüsselung verschlüsselt werden. Der Vorteil bei SSL ist, dass es ein Standardprotokoll ist und daher eine schnellere Verbindung aufgebaut werden kann als mit der SafeGuard Transportverschlüsselung.

  Mac: Um die Verbindung zwischen dem SafeGuard Enterprise Server und Mac Endpoints abzusichern, muss SSL verwendet werden.

  Hinweis: Wir empfehlen dringend, SSL-verschlüsselte Kommunikation zu verwenden, es sei denn, es handelt sich um Demo- oder Test-Installationen. Falls dies nicht möglich ist und die SafeGuard-spezifische Verschlüsselung verwendet wird, so gilt die Obergrenze von 1000 Clients, die eine Verbindung mit einer Serverinstanz herstellen können.

Bevor SSL für SafeGuard Enterprise aktiviert werden kann, muss eine funktionsfähige SSL-Umgebung eingerichtet werden.

7.1 Einrichten von SSL

Die folgenden allgemeinen Aufgaben müssen für die SSL-Einrichtung auf dem Web Server durchgeführt werden:

- Certificate Authority muss auf dem Server installiert sein, um die bei der SSL-Verschlüsselung verwendeten Zertifikate auszustellen.
- Ein Zertifikat muss ausgestellt und der IIS Server so konfiguriert werden, dass er SSL verwendet und auf das Zertifikat zeigt.
- Der Servername, den Sie bei der Konfiguration des SafeGuard Enterprise Servers angeben, muss identisch sein mit dem Servernamen, den Sie vorab im SSL-Zertifikat angegeben haben. Sonst können Client und Server nicht miteinander kommunizieren. Für jeden SafeGuard Enterprise Server wird ein separates SSL-Zertifikat benötigt.
- Wenn Sie Network Load Balancer einsetzen, vergewissern Sie sich, dass der Portbereich den SSL-Port mit einschließt.

Weitere Informationen erhalten Sie von unserem technischen Support oder hier:

- *http://msdn2.microsoft.com/en-us/library/ms998300.aspx*
- *http://support.microsoft.com/default.aspx?scid=kb;en-us;316898*

- *https://blogs.msdn.com/sql_protocols/archive/2005/11/10/491563.aspx*

7.2 Aktivieren der SSL-Verschlüsselung in SafeGuard Enterprise

So aktivieren Sie die SSL-Verschlüsselung in SafeGuard Enterprise:

- Verbindung zwischen Web Server und Datenbankserver:

  Aktivieren Sie SSL-Verschlüsselung während der Registrierung des SafeGuard Enterprise Servers im SafeGuard Management Center Konfigurationspakete-Werkzeug. Für weitere Informationen, siehe *Konfigurieren der Datenbankserver-Verbindung* (Seite 27) oder: *http://www.sophos.com/de-de/support/knowledgebase/109012.aspx*.

- Für die Verbindung zwischen Datenbankserver und SafeGuard Management Center

  Aktivieren Sie die SSL-Verschlüsselung im SafeGuard Management Center Konfigurationsassistenten, siehe *Konfigurieren der Datenbankserver-Verbindung* (Seite 27).

- Verbindung zwischen SafeGuard Enterprise Server und durch SafeGuard Enterprise geschützte Endpoints:

  Aktivieren Sie SSL-Verschlüsselung beim Erzeugen des Konfigurationspakets für den durch SafeGuard Enterprise verwalteten Endpoint im SafeGuard Management Center Konfigurationspakete-Werkzeug, siehe *Erzeugen eines Konfigurationspakets für zentral verwaltete Computer* (Seite 53). Nähere Informationen, wie SSL am SafeGuard Enterprise Server und dem durch SafeGuard Enterprise geschützten Endpoint zu konfigurieren ist, finden Sie unter *Sichern der Kommunikation zwischen Server und Endpoint mit SSL* (Seite 41).

Sie können die SSL-Verschlüsselung für SafeGuard Enterprise während der Erstkonfiguration der SafeGuard Enterprise Komponenten oder zu einem späteren Zeitpunkt einrichten. Erstellen Sie danach ein neues Konfigurationspaket und installieren Sie es auf dem entsprechenden Server oder zentral verwalteten Computer.

7.3 Sichern der Kommunikation zwischen Server und Endpoint mit SSL

7.3.1 Voraussetzungen

Um die Kommunikation zwischen dem SafeGuard Enterprise Server und dem mit SafeGuard Enterprise gesicherten Endpoint mit SSL zu sichern, ist ein gültiges Zertifikat notwendig. Sie können die folgenden Typen von Zertifikaten verwenden:

- Ein selbst-signiertes Zertifikat, siehe *Verwenden eines selbst-signierten Zertifikats* (Seite 42).
- Ein von einer PKI ausgestelltes Zertifikat mit einem privaten oder öffentlichen Stammzertifikat, siehe *Verwenden eines PKI-generierten Zertifikats* (Seite 43).

  Technisch macht es keinen Unterschied, ob Sie ein Zertifikat mit einem privaten oder öffentlichen Stammzertifikat verwenden.

Hinweis: Wenn nur ein von einer PKI erstelltes Zertifikat, aber keine PKI Infrastruktur verfügbar ist, können Sie das Zertifikat nicht verwenden, um die Kommunikation mit SSL zu sichern. In diesem Fall müssen Sie eine PKI aufsetzen oder ein selbst-signiertes Zertifikat erstellen.

7.3.2 Den SafeGuard Enterprise Server aufsetzen

Um den SafeGuard Enterprise Server so zu konfigurieren, dass er SSL für die Kommunikation zwischen Server und mit SafeGuard Enterprise geschütztem Endpoint verwendet, führen Sie die folgenden allgemeinen Schritte aus:

1. Installieren Sie das SafeGuard Management Center, siehe auch *Installieren des SafeGuard Management Center* (Seite 25).
2. Installieren Sie den SafeGuard Enterprise Server, siehe auch *Installieren von SafeGuard Enterprise Server* (Seite 15).
3. Testen Sie die Kommunikation zwischen SafeGuard Enterprise Server und der SQL-Datenbank mit dem Aufruf-Test.

Nachdem Sie diese Konfigurationsschritte erfolgreich abgeschlossen haben, importieren Sie das Zertifikat, das für die SSL Kommunikation verwendet werden soll. Sie können entweder ein selbst-signiertes Zertifikat oder ein bestehendes verwenden. Wenn Sie über eine PKI Infrastruktur verfügen, können Sie ein PKI-generiertes Zertifikat verwenden.

7.3.3 Verwenden eines selbst-signierten Zertifikats

Um ein selbst-signiertes Zertifikat mit SafeGuard Enterprise zu erstellen:

1. Öffnen Sie den Internetinformationsdienste (IIS) Manager auf dem Computer auf dem der SafeGuard Enterprise Server gehostet wird.
2. Überprüfen Sie den Namen des Servers, der am obersten Knoten angezeigt wird.
3. Auf dem Computer, auf dem das SafeGuard Management Center installiert ist, wählen Sie **Programme**, **Sophos**, **SafeGuard** und **SafeGuard Enterprise Zertifikatsverwaltung**.

   Die **SafeGuard Enterprise Zertifikatsverwaltung** wird angezeigt.

4. Geben Sie Ihr Kennwort ein, um den SafeGuard Zertifikatspeicher zu öffnen.
5. Klicken Sie die Schaltfläche **Neues Zertifikat erzeugen**.

   Der Dialog **Neues Zertifikat erzeugen** wird angezeigt.

6. Erstellen Sie ein neues Zertifikat:

   a) Der Zertifikatsname muss dem Computer entsprechen, der im Internetinformationsdienste (IIS) Manager im obersten Knoten angezeigt wird.

   b) Behalten Sie den Standardwert für die Schlüssellänge bei.

   c) Geben Sie nach Belieben ein Kennwort ein.

   d) Klicken Sie auf **OK**.

7. Speichern Sie die cert und p12 Dateien an einem Speicherort, der vom Computer erreichbar ist, auf dem der IIS installiert ist.

7.3.4 Verwenden eines PKI-generierten Zertifikats

Wollen Sie ein PKI-generiertes Zertifikat für die SSL-Kommunikation verwenden, erstellen Sie ein Zertifikat für den Computer, auf dem der SafeGuard Enterprise Server läuft. Die folgenden Anforderungen sind gegeben:

- Der Zertifikatsname muss dem Computer entsprechen, der im Internetinformationsdienste (IIS) Manager im obersten Knoten angezeigt wird.
- Der FQDN Name des Computers muss bei der Ausstellung des Zertifikats verwendet werden.

Hinweis: Wenn nur ein von einer PKI erstelltes Zertifikat, aber keine PKI Infrastruktur verfügbar ist, können Sie das Zertifikat nicht verwenden, um die Kommunikation mit SSL zu sichern. In diesem Fall müssen Sie eine PKI aufsetzen oder ein selbst-signiertes Zertifikat erstellen.

7.3.5 Konfigurieren der SGNSRV Webseite ein Zertifikat zu akzeptieren

Voraussetzung: Ein gültiges Zertifikat, um SSL zu verwenden, ist verfügbar.

Hinweis: Die folgende Beschreibung bezieht sich auf Microsoft Windows Server 2012.

1. Öffnen Sie den **Internetinformationsdienste (IIS) Manager**.
2. Im Navigationsbereich wählen Sie den Server, der die SGNSRV Webseite hostet.
3. Im Bereich rechts wählen Sie **Serverzertifikate** aus dem Abschnitt **IIS**.
4. Auf der Seite **Serverzertifikate** klicken Sie im Bereich **Aktionen** auf **Importieren...**
5. Wählen Sie das Zertifikat aus, das für die Sicherung der SSL Verbindung verwendet werden soll. Geben Sie das Kennwort ein und klicken Sie auf **OK**.
6. Klicken Sie im Navigationsbereich mit der rechten Maustaste auf **Default Web Site** und klicken Sie dann auf **Bindungen bearbeiten...**
7. Klicken Sie **Hinzufügen** im Dialog **Sitebindungen**.
8. Unter **Typ:** wählen Sie **https**, und unter **SSL-Zertifikat:** wählen Sie das Zertifikat, das für die Sicherung der SSL Verbindung verwendet werden soll.
9. Klicken Sie **OK** und schließen Sie den Dialog **Sitebindungen**.
10. Wählen Sie im Navigationsbereich den Server und klicken Sie auf **Neu starten** im Bereich **Aktionen**.

7.3.6 Den Endpoint für SSL konfigurieren

Um SSL auf einem mit SafeGuard Enterprise geschützten Endpoint zu verwenden, führen Sie die folgenden Schritte aus:

1. Weisen Sie das Zertifikat dem Client zu.

2. Erstellen Sie ein Client Konfigurationspaket, das SSL beinhaltet, siehe auch *Erzeugen eines Konfigurationspakets für zentral verwaltete Computer* (Seite 53).

7.3.6.1 Zuweisen eines Zertifikats

Es gibt verschiedene Möglichkeiten, ein Zertifikat einem Endpoint zuzuweisen. Eine davon ist, eine Microsoft Gruppenrichtlinie zu verwenden. Dies wird in diesem Abschnitt beschrieben. Falls Sie eine andere Methode verwenden wollen, stellen Sie sicher, dass das Zertifikat im Zertifikatspeicher des lokalen Computers abgelegt ist.

Zuweisen eines Zertifikats mittels Gruppenrichtlinie

1. Öffnen Sie die **Gruppenrichtlinienverwaltung**.
2. Suchen Sie ein existierendes oder erstellen Sie ein neues GPO (Gruppenrichtlinienobjekt), das die Zertifikatseinstellungen beinhalten soll. Versichern Sie sich, dass das GPO mit der Domain, Site oder Organisationseinheit verbunden ist, deren Benutzer von der Richtlinie betroffen sein sollen.
3. Klicken Sie auf das GPO und wählen Sie **Bearbeiten...**

   Der **Gruppenrichtlinienverwaltungs-Editor** öffnet sich und zeigt den aktuellen Inhalt des Richtlinienobjekts an.
4. Öffnen Sie im Navigationsbereich **Computerkonfiguration** > **Windows-Einstellungen** > **Sicherheitseinstellungen** > **Richtlinien für öffentliche Schlüssel** > **Vertrauenswürdige Herausgeber**.
5. Klicken Sie das **Aktionen** Menü und klicken Sie dann auf **Importieren...**.
6. Folgen Sie den Anweisungen im **Zertifikatimport-Assistent** um das Zertifikat zu finden und zu importieren.
7. Wenn das Zertifikat selbst-signiert ist und nicht auf ein Zertifikat zurückverfolgt werden kann, das im Zertifikatsspeicher **Vertrauenswürdigen Stammzertifizierungsstellen** liegt, dann müssen die das Zertifikat auch in diesen Zertifikatsspeicher kopieren. Klicken Sie auf **Vertrauenswürdige Stammzertifizierungsstellen** und wiederholen Sie die Schritte 5 und 6 um eine Kopie des Zertifikats in diesem Zertifikatsspeicher zu installieren.

8 Registrieren und Konfigurieren des SafeGuard Enterprise Server

Zur Implementierung der Informationen für die Kommunikation zwischen IIS Server, Datenbank und dem SafeGuard-geschützten Endpoint muss der SafeGuard Enterprise Server registriert und konfiguriert werden. Die Informationen werden in einem Server-Konfigurationspaket gespeichert.

Diesen Schritt führen Sie im SafeGuard Management Center durch. Der Workflow ist davon abhängig, ob der SafeGuard Enterprise Server auf demselben Computer wie das SafeGuard Management Center oder auf einem anderen Computer installiert ist.

Sie können auch weitere Eigenschaften festlegen. So lassen sich z. B. zusätzliche Sicherheitsbeauftragte für den ausgewählten Server hinzufügen. Sie können auch die Verbindung zur Datenbank konfigurieren.

8.1 Registrieren und Konfigurieren des SafeGuard Enterprise Server für den aktuellen Computer

Wenn Sie das SafeGuard Management Center und SafeGuard Enterprise Server auf dem Computer, mit dem Sie derzeit arbeiten, installiert haben, registrieren und konfigurieren Sie den SafeGuard Enterprise Server.

Hinweis: Wenn Multi Tenancy installiert ist, steht diese Option nicht zur Verfügung.

1. Starten Sie das SafeGuard Management Center.
2. Klicken Sie im **Extras** Menü auf **Konfigurationspakete**.
3. Wählen Sie die Registerkarte **Server** und klicken Sie auf **Diesen Computer zum SGN Server machen**.

   Das SafeGuard Enterprise Server Configuration Setup wird automatisch gestartet.

4. Übernehmen Sie in allen folgenden Dialogen die Standardeinstellungen.

Der SafeGuard Enterprise Server ist installiert. Ein Server-Konfigurationspaket mit der Bezeichnung **`<Server>.msi`** wird erstellt und direkt auf dem aktuellen Computer installiert. Die Serverinformationen werden in der Registerkarte **Server** angezeigt. Sie können zusätzliche Konfigurationsschritte durchführen.

Hinweis: Wenn Sie ein neues Server-Konfigurationspaket (MSI) auf dem SafeGuard Enterprise Server installieren möchten, deinstallieren Sie zunächst das veraltete Konfigurationspaket. Löschen Sie darüber hinaus den Local Cache manuell, so dass er mit den neuen Konfigurationsdaten (z. B. SSL-Einstellungen) aktualisiert werden kann. Installieren Sie dieses Konfigurationspaket auf dem Server.

8.2 Registrieren und Konfigurieren des SafeGuard Enterprise Servers für einen anderen Computer

Wenn der SafeGuard Enterprise Server auf einem anderen Computer als das SafeGuard Management Center installiert wurde, registrieren und konfigurieren Sie den SafeGuard Enterprise Server:

1. Starten Sie das SafeGuard Management Center.
2. Klicken Sie im **Extras** Menü auf **Konfigurationspakete**.
3. Wählen Sie die Registerkarte **Server** und klicken Sie auf **Hinzufügen**.
4. Klicken Sie unter **Serverregistrierung** auf die Schaltfläche [**...**], um das Maschinenzertifikat des Servers auszuwählen. Es wird bei der Installation des SafeGuard Enterprise Servers erzeugt. Sie finden es standardmäßig im Verzeichnis `MachCert` des SafeGuard Enterprise Server Installationsverzeichnisses. Es trägt den Dateinamen `<Computername>.cer`. Wenn der SafeGuard Enterprise Server auf einem anderen Computer als das SafeGuard Management Center installiert ist, muss diese .cer-Datei als Kopie oder Netzwerkfreigabe zugreifbar sein.

   Wählen Sie nicht das MSO-Zertifikat.

   Der Fully Qualified Name (FQDN), z. B. `server.mycompany.com`, sowie Zertifikatsinformationen werden angezeigt.

   Hinweis: Wenn SSL als Transportverschlüsselung zwischen Endpoint und Server verwendet werden soll, muss der Servername, den Sie hier eingeben, mit dem Servernamen übereinstimmen, den Sie im SSL-Zertifikat vergeben haben. Andernfalls ist keine Kommunikation möglich.

5. Klicken Sie auf **OK**.

   Die Serverinformationen werden in der Registerkarte **Server** angezeigt.

6. Klicken Sie auf die Registerkarte **Server-Pakete**. Hier werden alle verfügbaren Server angezeigt. Wählen Sie dort den gewünschten Server aus. Geben Sie einen Ausgabepfad für das Konfigurationspaket an. Klicken Sie auf **Konfigurationspaket erstellen**.

   Ein Server-Konfigurationspaket (MSI) mit der Bezeichnung `<Server>.msi` wird im angegebenen Ausgabeort erstellt.

7. Bestätigen Sie die Erfolgsmeldung mit **OK**.
8. Klicken Sie in der Registerkarte **Server** auf **Schließen**.

Die Registrierung und Konfiguration des SafeGuard Enterprise Servers ist beendet. Installieren Sie das Server-Konfigurationspaket (MSI) auf dem Computer, auf dem der SafeGuard Enterprise Server läuft. Sie können die Serverkonfiguration in der Registerkarte **Server** jederzeit ändern.

Hinweis: Wenn Sie ein neues Server-Konfigurationspaket (MSI) auf dem SafeGuard Enterprise Server installieren möchten, deinstallieren Sie zunächst das veraltete Konfigurationspaket. Löschen Sie darüber hinaus den Local Cache manuell, so dass er mit den neuen Konfigurationsdaten (z. B. SSL-Einstellungen) aktualisiert werden kann. Installieren Sie dieses Konfigurationspaket auf dem Server.

8.3 Ändern der SafeGuard Enterprise Server Eigenschaften

Sie können die Eigenschaften und Einstellungen für jeden registrierten Server und seine Datenbankverbindung jederzeit ändern.

1. Wählen Sie den gewünschten Server in der Registerkarte **Server** des SafeGuard Management Center **Konfigurationspakete** Werkzeugs.
2. Gehen Sie wie folgt vor:

Element	Beschreibung
Skript ausführen	Klicken Sie hier, um die Verwendung von SafeGuard Enterprise Management API zu ermöglichen. Dies ermöglicht die Ausführung von administrativen Aufgaben über Skripte
Server-Rollen	Klicken Sie hier, um eine verfügbare Sicherheitsbeauftragtenrolle für den ausgewählten Server zu aktivieren/deaktivieren.
Server-Rolle hinzufügen...	Klicken Sie hier, um weitere spezifische Sicherheitsbeauftragtenrollen für den ausgewählten Server hinzuzufügen, falls erforderlich. Sie werden dazu aufgefordert, das Serverzertifikat auszuwählen. Die Sicherheitsbeauftragtenrolle wird hinzugefügt und kann unter **Server-Rollen** angezeigt werden.
Datenbankverbindung	Klicken Sie auf **[...]**, um die Verbindung zur Datenbank für jeden registrierten Server zu konfigurieren. Hier können Sie auch die Anmeldeinformationen für die Datenbank und die Transportverschlüsselung zwischen Web Server und Datenbankserver festlegen. Für weitere Informationen, siehe *Konfigurieren der Datenbankserver-Verbindung* (Seite 27). Selbst wenn die Prüfung der Datenbankverbindung nicht erfolgreich ist, kann ein neues Server-Konfigurationspaket erstellt werden. **Hinweis:** Sie müssen nicht den SafeGuard Management Center Konfigurationsassistenten erneut ausführen, um die Datenbankkonfiguration zu aktualisieren. Erstellen Sie einfach ein neues Server-Konfigurationspaket und verteilen Sie es an den entsprechenden Server. Sobald dieses auf dem Server installiert ist, kann auf die neue Datenbankverbindung zugegriffen werden.

3. Erstellen Sie ein neues Server-Konfigurationspaket in der Registerkarte **Server-Pakete**.
4. Deinstallieren Sie das veraltete Server-Konfigurationspaket und installieren Sie danach das neue auf dem entsprechenden Server.

Die neue Server-Konfiguration wird aktiv.

8.4 Registrieren des SafeGuard Enterprise Servers mit aktivierter Sophos Firewall

Ein durch SafeGuard Enterprise geschützter Endpoint kann keine Verbindung mit dem SafeGuard Enterprise Server herstellen, wenn eine Sophos Firewall mit Standardeinstellungen auf dem Endpoint installiert ist. Die Sophos Firewall sperrt standardmäßig NetBIOS-Verbindungen, die für die Auflösung des Netzwerknamens des SafeGuard Enterprise Servers benötigt werden.

1. Führen Sie als Workaround einen der folgenden Schritte aus:
   - Geben Sie die NetBIOS-Verbindungen in der Firewall frei.
   - Fügen Sie den Fully Qualified Name des SafeGuard Enterprise Servers im Konfigurationspaket hinzu. Für weitere Informationen, siehe *Registrieren und Konfigurieren des SafeGuard Enterprise Servers für einen anderen Computer* (Seite 46).

9 Einrichten von SafeGuard Enterprise auf Endpoints

Die SafeGuard Enterprise Verschlüsselungssoftware fügt sich nahtlos in die gewohnte Benutzerumgebung ein und lässt sich leicht und intuitiv bedienen. Je nach Ihrer Strategie für den Einsatz von SafeGuard Enterprise können Sie die Endpoints mit verschiedenen SafeGuard Enterprise Modulen ausstatten und sie gemäß Ihren Anforderungen konfigurieren.

Sicherheitsbeauftragte können die Installation und Konfiguration lokal auf den Endpoints oder im Rahmen einer zentralisierten Software-Installation ausführen. Durch eine zentrale Installation wird eine standardisierte Installation auf mehreren Endpoints erreicht.

9.1 Zentral verwaltete Endpoints und Standalone-Endpoints

Endpoints können folgendermaßen konfiguriert werden:

- **Zentral verwaltet - SafeGuard Enterprise Clients (Managed)**

  Zentrale, server-basierte Verwaltung im SafeGuard Management Center

  Für zentral verwaltete Endpoints besteht generell eine Verbindung zum SafeGuard Enterprise Server. Sie erhalten ihre Richtlinien über den SafeGuard Enterprise Server. Die Verbindung kann temporär unterbrochen sein, z. B. während einer Geschäftsreise. Trotzdem ist der Endpoint auch in dieser Situation als zentral verwaltet definiert.

- **Standalone - Sophos SafeGuard Clients (Standalone)**

  Lokale Verwaltung durch im SafeGuard Management Center erstellte Konfigurationspakete.

  Für Standalone-Endpoints besteht nie eine Verbindung zum SafeGuard Enterprise Server. Damit fehlt die Verbindung zur zentralen Verwaltung von SafeGuard Enterprise. Sie werden im Standalone-Modus betrieben.

  Standalone-Endpoints erhalten SafeGuard Enterprise Richtlinien über Konfigurationspakete. Diese Computer erhalten Richtlinien nie über eine Verbindung zum SafeGuard Enterprise Server.

  SafeGuard Enterprise Richtlinien werden im SafeGuard Management Center erstellt und in Konfigurationspakete exportiert. Die Verteilung der Konfigurationspakete kann über firmeneigene Software-Verteilungsmechanismen erfolgen, oder das Konfigurationspaket wird manuell auf den Endpoints installiert.

Für die verschiedenen Endpoint-Typen stehen unterschiedliche Pakete und Module zur Verfügung.

9.2 Einschränkungen

Beachten Sie die in den folgenden Abschnitten beschriebenen Einschränkungen für SafeGuard Enterprise auf Endpoints.

9.2.1 Einschränkungen für zentral verwaltete Endpoints

Beachten Sie folgende Einschränkungen für zentral verwaltete Endpoints.

- **Einschränkungen für die Initialverschlüsselung**

  Im Rahmen der initialen Konfiguration von zentral verwalteten Endpoints können Verschlüsselungsrichtlinien erstellt werden, die in einem Konfigurationspaket an die durch SafeGuard Enterprise geschützten Endpoints verteilt werden können.

  Wenn der durch SafeGuard Enterprise geschützte Endpoint jedoch nicht direkt nach der Installation des Konfigurationspakets eine Verbindung mit dem SafeGuard Enterprise Server herstellt, sondern vorübergehend offline ist, werden nur Verschlüsselungsrichtlinien mit den folgenden spezifischen Einstellungen sofort wirksam:

  Geräteschutz vom Typ volume-basierend unter Anwendung des **definierten Computerschlüssels** als Verschlüsselungsschlüssel

  Damit alle anderen Richtlinien, die Verschlüsselung mit benutzerdefinierten Schlüsseln umfassen, auf dem durch SafeGuard Enterprise geschützten Endpoint wirksam werden, muss das entsprechende Konfigurationspaket auch noch einmal der Organizational Unit des Endpoint zugewiesen werden. Die benutzerdefinierten Schlüssel werden dann erst erstellt, wenn der Endpoint wieder eine Verbindung zum SafeGuard Enterprise Server hergestellt hat.

  Ursache hierfür ist, dass der **definierte Computerschlüssel** direkt auf dem durch SafeGuard Enterprise geschützten Endpoint beim ersten Neustart nach der Installation erstellt wird. Benutzerdefinierte Schlüssel hingegen können nur auf dem Endpoint erstellt werden, wenn er beim SafeGuard Enterprise Server registriert wurde.

- **Einschränkungen für die Unterstützung von BitLocker Drive Encryption**

  Das SafeGuard Data Exchange Paket (SGNClient_withoutDE.msi/SGNClient_withoutDE_x64.msi) steht für die Anwendung mit BitLocker Drive Encryption Unterstützung nicht zur Verfügung.

  Hinweis: Es kann entweder die SafeGuard Enterprise Festplattenverschlüsselung oder die BitLocker-Laufwerkverschlüsselung verwendet werden. Die gleichzeitige Verwendung beider Verschlüsselungstypen ist nicht möglich. Wenn Sie den Verschlüsselungstyp ändern möchten, müssen Sie zuerst alle verschlüsselten Laufwerke entschlüsseln, die SafeGuard Enterprise Verschlüsselungssoftware deinstallieren und dann mit den gewünschten Features neu installieren. Der Installer verhindert die gleichzeitige Installation beider Features.

  Das trifft auch dann zu, wenn kein Konfigurationspaket, das eine Verschlüsselung auslösen soll, installiert wurde. In diesem Fall müssen Sie ebenfalls die SafeGuard Enterprise Verschlüsselungssoftware deinstallieren und anschließend mit den gewünschten Features neu installieren.

9.2.2 Einschränkungen für Standalone-Endpoints

Die folgenden Features werden für Standalone-Endpoints (Sophos SafeGuard Clients Standalone) nicht unterstützt:

- File Share

9.3 Vorbereiten der Endpoints für die Verschlüsselung

Vor der Installation von SafeGuard Enterprise empfehlen wir folgende vorbereitende Maßnahmen.

- Auf dem Endpoint muss ein Benutzerkonto eingerichtet und aktiv sein.
- Stellen Sie sicher, dass Sie über Windows Administratorrechte verfügen.
- Erstellen Sie einen kompletten Backup Ihrer Daten auf dem Endpoint.
- Laufwerke, die verschlüsselt werden sollen, müssen komplett formatiert sein und einen Laufwerksbuchstaben zugewiesen haben.
- Sophos stellt eine Datei für die Hardware-Konfiguration zur Verfügung, um Konflikte zwischen der POA und Ihrer Endpoitn-Hardware zu vermeiden. Die Datei ist im Installationspaket der Verschlüsselungssoftware enthalten. Wir empfehlen, vor jeder größer angelegten SafeGuard Enterprise Installation die aktuelle Version dieser Datei zu installieren. Die Datei wird monatlich aktualisiert und steht hier zum Download zur Verfügung: *http://de.sophos.com/support/knowledgebase/65700.aspx*

  Sie können uns bei der Optimierung der Hardware-Kompatibilität unterstützen, indem Sie ein von uns zur Verfügung gestelltes Tool ausführen. Dieses Tool liefert ausschließlich Hardware-relevante Informationen. Das Tool ist einfach zu bedienen. Die gesammelten Informationen werden zur Hardware-Konfigurationsdatei hinzugefügt. Für weitere Informationen, siehe *http://www.sophos.com/de-de/support/knowledgebase/110285.aspx*.

- Untersuchen Sie die Festplatte(n) mit folgendem Kommando auf Fehler:

  ```
  chkdsk %drive% /F /V /X
  ```

  Unter Umständen werden Sie dazu aufgefordert, den Endpoint neu zu starten und `chkdsk` noch einmal auszuführen. Weitere Informationen finden Sie unter: *http://www.sophos.com/de-de/support/knowledgebase/107799.aspx*.

  So prüfen Sie die Ergebnisse (Log-Datei) in der Windows-Ereignisanzeige:

    Windows 7: Wählen Sie **Windows Logs**, **Anwendung**, **Wininit**.

- Benutzen Sie das Windows-Tool "defrag", um fragmentierte Boot-Dateien, Datendateien und Ordner auf lokalen Volumes aufzufinden und zu konsolidieren. Weitere Informationen finden Sie unter: *http://www.sophos.com/de-de/support/knowledgebase/109226.aspx*.
- Deinstallieren Sie Third-Party Boot-Manager, z. B. PROnetworks Boot Pro und Boot-US.

- Wir empfehlen, vor jeder größer angelegten SafeGuard Enterprise Installation die aktuelle Version der POA-Konfigurationsdatei zu installieren. Die Datei wird monatlich aktualisiert und steht hier zum Download zur Verfügung: *http://www.sophos.com/de-de/support/knowledgebase/657000.aspx*.

- Wenn die Bootpartition auf dem Endpoint von FAT nach NTFS konvertiert wurde, der Endpoint aber noch nicht neu gestartet wurde, sollten Sie den Endpoint einmal neu starten. Andernfalls kann die Installation unter Umständen nicht erfolgreich abgeschlossen werden.

- Nur für SafeGuard Enterprise Clients (managed): Kontrollieren Sie, ob eine Verbindung zum SafeGuard Enterprise Server besteht. Rufen Sie auf den Endpoints im Internet Explorer folgende Web-Adresse auf: http://<ServerIPAddress>/sgnsrv. Wenn die **Trans**-Seite mit dem Eintrag **Check Connection** erscheint, ist die Verbindung zum SafeGuard Enterprise Server hergestellt.

9.3.1 Vorbereitung für Cloud Storage

Das SafeGuard Enterprise Modul Cloud Storage bietet dateibasierende Verschlüsselung von in der Cloud gespeicherten Daten.

Cloud Storage stellt sicher, dass die lokalen Kopien von Cloud-Daten transparent verschlüsselt werden und auch verschlüsselt bleiben, wenn sie in der Cloud gespeichert werden.

Die Art und Weise, wie Benutzer mit in der Cloud gespeicherten Daten arbeiten, wird dadurch nicht beeinflusst. Auf die anbieterspezifische Cloud-Software hat die Anwendung des Moduls keine Auswirkungen. Sie kann wie zuvor zum Übertragen von Daten an die Cloud oder zum Empfangen von Daten aus der Cloud benutzt werden.

So bereiten Sie Ihre Endpoints für Cloud Storage vor:

- Die anbieterspezifische Cloud Storage Software muss auf den Endpoint-Computern, auf denen Sie das Modul Cloud Storage installieren möchten, installiert sein.

- Die anbieterspezifische Cloud Storage Software muss eine Anwendung oder einen Systemdienst im lokalen Dateisystem für die Synchronisierung zwischen der Cloud und dem lokalen System enthalten.

- Die anbieterspezifische Cloud Storage Software muss die synchronisierten Daten im lokalen Dateisystem speichern.

Hinweis: Cloud Storage verschlüsselt nur neue in der Cloud gespeicherte Daten. Wurden Daten bereits vor der Installation von Cloud Storage in der Cloud gespeichert, so werden diese Daten nicht automatisch verschlüsselt. Um diese Daten zu verschlüsseln, müssen die Benutzer sie zunächst aus der Cloud entfernen und sie nach der Installation von Cloud Storage wieder an die Cloud übergeben.

9.3.2 Vorbereitung für die Unterstützung von BitLocker Drive Encryption

Hinweis: Bevor Sie mit der Installation beginnen, entscheiden Sie, ob Sie SafeGuard Enterprise in Verbindung mit der BitLocker Drive Encryption oder die native SafeGuard Enterprise Festplattenverschlüsselung anwenden möchten. Wenn Sie versuchen, beides gleichzeitig zu installieren, wird die Installation abgebrochen.

Wenn Sie mit SafeGuard Enterprise BitLocker Endpoints verwalten möchten, treffen Sie folgende spezifische vorbereitende Maßnahmen auf dem Endpoint:

- Auf dem Endpoint muss Windows 7 oder Windows 8 installiert sein.
- BitLocker Drive Encryption muss installiert und aktiviert sein.
- Wenn TPM für die Authentisierung verwendet werden soll, muss TPM initialisiert, im Besitz und aktiviert sein.
- Wenn Sie die volume-basierende Verschlüsselung von SafeGuard Enterprise installieren möchten, sollten Sie sicherstellen, dass die Volumes nicht bereits mit BitLocker Drive Encryption verschlüsselt wurden. Andernfalls kann es zu einer Beschädigung des Systems kommen.
- Um die BitLocker Drive Encryption Unterstützung zu installieren, deaktivieren Sie entweder User Access Control (UAC) oder melden Sie sich mit dem integrierten Administrator-Benutzerkonto an.

9.3.3 Vorbereiten einer "Ändern"-Installation

Wenn Sie eine vorhandene SafeGuard Enterprise Installation ändern oder bestimmte Module zu einem späteren Zeitpunkt installieren, meldet das Installationsprogramm u. U., dass bestimmte Komponenten (z. B. SafeGuard Removable Media Manager) derzeit benutzt werden. Diese Meldung wird dadurch verursacht, dass diese Module gemeinsame Komponenten benutzen, die derzeit verwendet werden und daher nicht sofort aktualisiert werden können. Diese Meldung kann ignoriert werden, da die betroffenen Komponenten beim Neustart des Computers ohnehin aktualisiert werden.

Dieses Verhalten gilt für die Installation in überwachtem und nicht überwachtem Modus.

9.4 Erzeugen von Konfigurationspaketen

Erzeugen Sie je nach erforderlicher Konfiguration die passenden Konfigurationspakete für die Endpoints im SafeGuard Management Center:

- Für zentral verwaltete Windows Endpoints - Pakete für Managed Clients
- Für Standalone Windows Endpoints - Pakete für Standalone Clients
- Für Macs - Pakete für Managed Clients
- Wenn Sie Service Accounts für Aufgaben nach der Installation verwenden.

Das erste Konfigurationspaket muss auf den Endpoints zusammen mit der Verschlüsselungssoftware installiert werden.

9.4.1 Erzeugen eines Konfigurationspakets für zentral verwaltete Computer

1. Klicken Sie im SafeGuard Management Center im **Extras** Menü auf **Konfigurationspakete**.
2. Wählen Sie **Pakete für Managed Clients**.

3. Klicken Sie auf **Konfigurationspaket hinzufügen**.
4. Geben Sie einen beliebigen Namen für das Konfigurationspaket ein.
5. Ordnen Sie einen primären SafeGuard Enterprise Server zu (der sekundäre Server ist nicht notwendig).
6. Falls erforderlich, geben Sie eine Richtliniengruppe an, die auf die Computer angewendet werden soll. Diese müssen Sie zuvor im SafeGuard Management Center erstellt haben. Wenn Sie für Aufgaben nach der Installation auf dem Computer Service Accounts verwenden möchten, stellen Sie sicher, dass die entsprechende Richtlinieneinstellung in dieser ersten Richtliniengruppe definiert ist, siehe *Service Accounts für die Durchführung von Aufgaben nach der Installation* (Seite 56).
7. Wählen Sie den Modus für die **Transportverschlüsselung**, der bestimmt, wie die Verbindung zwischen SafeGuard Enterprise Client und SafeGuard Enterprise Server verschlüsselt wird: Sophos-Verschlüsselung oder SSL-Verschlüsselung.

   Der Vorteil bei SSL ist, dass es ein Standardprotokoll ist und eine schnellere Verbindung aufgebaut werden kann als mit der SafeGuard Transportverschlüsselung. SSL-Verschlüsselung wird standardmäßig ausgewählt. Für weitere Informationen, siehe *Sichern von Transportverbindungen mit SSL* (Seite 40).
8. Geben Sie einen Ausgabepfad für das Konfigurationspaket (MSI) an.
9. Klicken Sie auf **Konfigurationspaket erstellen**.

   WennSie als Modus für die **Transportverschlüsselung** die SSL-Verschlüsselung ausgewählt haben, wird die Serververbindung validiert. Wenn die Verbindung fehlschlägt, wird eine Warnungsmeldung angezeigt.

Das Konfigurationspaket (MSI) wird im angegebenen Verzeichnis angelegt. Im nächsten Schritt verteilen Sie das Paket an die Endpoints zur Installation.

9.4.2 Erzeugen eines Konfigurationspakets für Standalone-Computer

1. Klicken Sie im SafeGuard Management Center im **Extras** Menü auf **Konfigurationspakete**.
2. Wählen Sie **Pakete für Standalone Clients**.
3. Klicken Sie auf **Konfigurationspaket hinzufügen**.
4. Geben Sie einen beliebigen Namen für das Konfigurationspaket ein.
5. Geben Sie eine zuvor im SafeGuard Management Center erstellte **Richtliniengruppe** an, die für die Computer gelten soll.

6. Geben Sie unter **Speicherort für Schlüssel-Sicherungskopie** einen freigegebenen Netzwerkpfad für das Speichern der Schlüssel-Recovery-Datei an oder wählen Sie einen Netzwerkpfad aus. Geben Sie den freigegebenen Pfad in folgender Form ein: **`\\network computer\`**, zum Beispiel **`\\mycompany.edu\`**. Wenn Sie hier keinen Pfad angeben, wird der Benutzer beim ersten Anmelden am Endpoint nach der Installation gefragt, wo die Schlüsseldatei gespeichert werden soll.

   Die Schlüssel-Recovery-Datei (XML) wird für die Durchführung von Recovery-Vorgängen bei durch Sophos SafeGuard geschützten Computern benötigt. Sie wird auf allen durch Sophos SafeGuard geschützten Computern erzeugt.

   Hinweis: Stellen Sie sicher, dass diese Schlüssel-Recovery-Datei an einem Speicherort abgelegt wird, auf den die Mitarbeiter des Helpdesk Zugriff haben. Die Dateien können dem Helpdesk auch durch andere Mechanismen zugänglich gemacht werden. Die Datei ist mit dem Unternehmenszertifikat verschlüsselt. Sie kann also auch auf externen Medien oder auf dem Netzwerk gespeichert werden, um sie dem Helpdesk für Recovery-Vorgänge zur Verfügung zu stellen. Sie kann auch per E-Mail verschickt werden.

7. Unter **POA Gruppe** können Sie eine POA-Gruppe auswählen, die dem Endpoint zugeordnet wird. POA-Benutzer können für administrative Aufgaben auf den Endpoint zugreifen, nachdem die Power-on Authentication aktiviert wurde. Um POA-Benutzer zuzuweisen, müssen Sie die POA-Gruppe zunächst im Bereich **Benutzer & Computer** des SafeGuard Management Center anlegen.
8. Geben Sie einen Ausgabepfad für das Konfigurationspaket (MSI) an.
9. Klicken Sie auf **Konfigurationspaket erstellen**.

Das Konfigurationspaket (MSI) wird im angegebenen Verzeichnis angelegt. Im nächsten Schritt verteilen Sie das Paket an die Endpoints zur Installation.

9.4.3 Erzeugen eines Konfigurationspakets für Macs

Ein Konfigurationspaket für einen Mac enthält die relevanten Serverinformationen sowie das Unternehmenszertifikat. Der Mac benutzt diese Informationen zum Zurückmelden von Statusinformationen (z. B. POA an/aus, Verschlüsselungsstatus). Die Statusinformationen werden im SafeGuard Management Center angezeigt.

1. Klicken Sie im SafeGuard Management Center im **Extras** Menü auf **Konfigurationspakete**.
2. Wählen Sie **Pakete für Managed Clients**.
3. Klicken Sie auf **Konfigurationspaket hinzufügen**.
4. Geben Sie einen beliebigen Namen für das Konfigurationspaket ein.
5. Ordnen Sie einen primären SafeGuard Enterprise Server zu (der sekundäre Server ist nicht notwendig).
6. Wählen Sie **SSL** als **Transportverschlüsselung** für die Verbindung zwischen dem Endpoint und dem SafeGuard Enterprise Server. Für Macs wird **Sophos** als **Transportverschlüsselung** nicht unterstützt.
7. Geben Sie einen Ausgabepfad für das Konfigurationspaket (ZIP) an.
8. Klicken Sie auf **Konfigurationspaket erstellen**.

   Die Server-Verbindung für den SSL **Transportverschlüsselung** Modus wird validiert. Wenn die Verbindung fehlschlägt, wird eine Warnungsmeldung angezeigt.

Das Konfigurationspaket (ZIP) wird nun im angegebenen Verzeichnis angelegt. Im nächsten Schritt verteilen Sie das Paket an Ihre Macs zur Installation.

9.4.4 Service Accounts für die Durchführung von Aufgaben nach der Installation

Wenn Sie SafeGuard Enterprise über einen zentralen Rollout-Vorgang installieren möchten, empfehlen wir die Konfiguration einer Service Account-Liste. Ein IT-Administrator, der zu einer Service Account-Liste hinzugefügt wurde, kann sich nach der Installation von SafeGuard Enterprise an Endpoints anmelden, ohne die Power-on Authentication zu aktivieren. Ein solches Vorgehen ist empfehlenswert, da normalerweise der erste Benutzer, der sich nach der Installation an einem Endpoint anmeldet, als primäres Benutzerkonto zur POA hinzugefügt wird. Die in den Listen enthaltenen Benutzer werden als SafeGuard Enterprise Gastbenutzer behandelt.

Mit Service Accounts ergibt sich folgender Workflow:

- SafeGuard Enterprise wird auf einem Endpoint installiert.
- Der Endpoint wird neu gestartet und ein Rollout-Beauftragter, der in einer Service Account Liste aufgeführt ist, meldet sich über die Windows-Eingabe-Aufforderung an.
- Gemäß der auf den Endpoint angewendeten Service Account Liste wird der Benutzer als Service Account erkannt und als Gastbenutzer behandelt.
- Der Rollout-Beauftragte wird nicht zur POA hinzugefügt und die POA wird nicht aktiviert. Der Endbenutzer kann sich anmelden und die POA aktivieren.

Hinweis: Service Account Listen müssen Sie in einer Richtlinie anlegen und diese der ersten Richtliniengruppe des ersten Konfigurationspakets zuweisen, das Sie nach der Installation der Verschlüsselungssoftware auf dem Endpoint installieren. Weitere Informationen hierzu finden Sie in der *SafeGuard Enterprise Administrator-Hilfe*.

9.5 Installation der Verschlüsselungssoftware

Für das Einrichten der SafeGuard Enterprise Verschlüsselungssoftware auf Endpoints gibt es zwei Möglichkeiten:

- Lokales Installieren der Verschlüsselungssoftware Dies ist zum Beispiel für eine Testinstallation empfehlenswert.
- Zentrales Installieren der Verschlüsselungssoftware Dadurch wird eine standardisierte Installation auf mehreren Endpoints erreicht.

Bevor Sie mit der Installation beginnen, prüfen Sie die verfügbaren Installationspakete und Features für zentral verwaltete Endpoints und Standalone-Endpoints. Die Installationsschritte für beide Varianten sind identisch, mit der Ausnahme, dass für jeden der beiden ein unterschiedliches Konfigurationspaket zugeordnet werden muss.

Das Verhalten des Endpoint bei der ersten Anmeldung nach der Installation von SafeGuard Enterprise und der Aktivierung der Power-on Authentication ist in der *SafeGuard Enterprise Benutzerhilfe* beschrieben.

9.5.1 Installationspakete und Features

Die folgende Tabelle zeigt die Installationspakete und Features der Sophos SafeGuard Verschlüsselungssoftware auf Endpoints. Sie finden die Installationspakete im Installers Ordner Ihrer Produktlieferung.

Hinweis: Wenn das Betriebssystem des Endpoints 64-Bit ist, können Sie die 64-Bit-Variante der Installationspakete (<Paketname>_x64.msi) installieren.

Es ist zwar möglich, bei einer Erstinstallation nicht alle Features zu installieren, wir empfehlen jedoch, das komplette SafeGuard Paket für die Festplattenverschlüsselung von Beginn an zu installieren.

Paket	Inhalt	Verfügbar für zentral verwaltete Endpoints	Verfügbar für Standalone Endpoints
SGxClientPreinstall.msi	**Prä-Installations-Paket** Dieses Paket muss vor der Installation eines Verschlüsselungsinstallationspakets installiert werden. Es stattet Endpoints mit notwendigen Voraussetzungen für eine erfolgreiche Installation der aktuellen Verschlüsselungssoftware aus.	Obligatorisch	Obligatorisch
SGNClient.msi SGNClient_x64.msi	**SafeGuard Paket für die Festplattenverschlüsselung**		
	BaseEncryption, SectorBasedEncryption Festplattenverschlüsselung für interne und externe Festplatten. Mit Power-on Authentication Wählen Sie den Installationstyp **Vollständig**, **Typisch** oder **Angepasst**.		
	BitLockerSupport BitLocker Drive Encryption mit SafeGuard Enterprise Unterstützung. Erfordert Microsoft BitLocker. Wählen Sie den Installationstyp **Angepasst**.	Es kann entweder **SectorBasedEncryption** ODER **BitLockerSupport** installiert werden.	

Paket	Inhalt	Verfügbar für zentral verwaltete Endpoints	Verfügbar für Standalone Endpoints
	SecureDataExchange SafeGuard Data Exchange: Dateibasierende Verschlüsselung von Daten auf Wechselmedien auf allen Plattformen ohne Neuverschlüsselung. Wählen Sie den Installationstyp **Vollständig** oder **Angepasst**.	✓	✓
	FileShare Dateibasierende Verschlüsselung von Daten auf lokalen Festplatten und Netzwerkfreigaben, speziell für Arbeitsgruppen. Wählen Sie den Installationstyp **Vollständig** oder **Angepasst**.	✓	✗
	CloudStorage Dateibasierende Verschlüsselung für in der Cloud gespeicherte Daten. Lokale Kopien von in der Cloud gespeicherten Daten werden stets transparent verschlüsselt. Für das Übertragen von Daten an die Cloud oder den Empfang von Daten aus der Cloud muss anbieterspezifische Software benutzt werden. Wählen Sie den Installationstyp **Vollständig** oder **Angepasst**.	✓	✓
SGNClient_withoutDE.msi SGNClient_withoutDE_x64.msi	**Dateibasierende Verschlüsselung**		
	SecureDataExchange SafeGuard Data Exchange: Dateibasierende Verschlüsselung von Daten auf Wechselmedien auf allen Plattformen ohne Neuverschlüsselung Es steht keine Power-on Authentication zur Verfügung. Wählen Sie den Installationstyp **Vollständig, Typisch** oder **Angepasst**.	✓	✓

Paket	Inhalt	Verfügbar für zentral verwaltete Endpoints	Verfügbar für Standalone Endpoints
	FileShare Dateibasierende Verschlüsselung von Daten auf lokalen Festplatten und Netzwerkfreigaben, speziell für Arbeitsgruppen. Wählen Sie den Installationstyp **Vollständig** oder **Angepasst**.	✓	✗
	CloudStorage Dateibasierende Verschlüsselung für in der Cloud gespeicherte Daten. Lokale Kopien von in der Cloud gespeicherten Daten werden stets transparent verschlüsselt. Für das Übertragen von Daten an die Cloud oder den Empfang von Daten aus der Cloud muss anbieterspezifische Software benutzt werden. Wählen Sie den Installationstyp **Vollständig** oder **Angepasst**.	✓	✓
SGNClientRuntime.msi SGNClientRuntime_x64.msi	**SafeGuard Runtime Paket** Ermöglicht das Starten des Endpoint von einem sekundären Boot-Laufwerk ermöglicht, wenn mehrere Betriebssysteme installiert sind und der den Zugriff auf diese Laufwerke erlaubt, wenn diese durch die primäre SafeGuard Enterprise Installation verschlüsselt sind.	✓	✓

9.5.2 Lokales Installieren der Verschlüsselungssoftware

Voraussetzungen:

- Die Endpoints müssen für die Verschlüsselung vorbereitet sein, siehe *Vorbereiten der Endpoints für die Verschlüsselung* (Seite 51).
- Entscheiden Sie, welches Verschlüsselungspaket und welche Features installiert werden sollen.

So führen Sie eine lokale Installation der Verschlüsselungssoftware durch:

1. Melden Sie sich an dem Endpoint als Administrator an.
2. Wenn Sie auf einem Endpoint LAN Crypt 3.7x installiert haben und SafeGuard Data Exchange installieren möchten, installieren Sie zuerst die Kompatibilitätskomponente `SGFileEncCompLayer.msi` oder `SGFileEncCompLayer_x64.msi`. Sie finden die Komponente in Ihrer Produktlieferung. Für weitere Informationen, siehe *Kompatibilität mit SafeGuard LAN Crypt* (Seite 10).
3. Installieren Sie das aktuelle Prä-Installationspaket **`SGxClientPreinstall.msi`**, das den Endpoint mit den nötigen Voraussetzungen für eine erfolgreiche Installation der aktuellen Verschlüsselungssoftware ausstattet.

   Hinweis: Alternativ können Sie auch die Datei **`vcredist_x86.exe`** installieren, die Sie hier herunterladen können:
   http://www.microsoft.com/downloads/details.aspx?FamilyID=766a6af7-ec73-40ff-b072-9112bab119c2
   oder stellen Sie sicher, dass **`MSVCR100.dll`** im Ordner Windows\WinSxS folder auf dem Computer vorhanden ist.

4. Doppelklicken Sie auf dem relevanten Verschlüsselungssoftwarepaket (MSI). Ein Assistent führt Sie durch die notwendigen Schritte.
5. Übernehmen Sie im Assistenten in allen folgenden Dialogen die Standardeinstellungen.

   Hinweis: Bei einer Erstinstallation empfehlen wir, von Beginn an eine **Vollständige** Installation auszuwählen. Um nur einen Teil der Features zu installieren, wählen Sie eine **Angepasste** Installation und aktivieren/deaktivieren Sie die entsprechenden Features.

   SafeGuard Enterprise wird auf dem Endpoint installiert.

6. Wechseln Sie an den Speicherort des relevanten Konfigurationspakets (MSI), das Sie zuvor im SafeGuard Management Center erzeugt haben. Für zentral verwaltete Endpoints und Standalone-Endpoints müssen spezifische Konfigurationspakete installiert werden, siehe *Erzeugen von Konfigurationspaketen* (Seite 53).
7. Installieren Sie das relevante Konfigurationspaket (MSI) auf dem Computer.
8. Stellen Sie nach der Installation sicher, dass die Endpoints zweimal neu gestartet werden, um die Power-on Authentication zu aktivieren. Die Computer müssen ein drittes Mal neu gestartet werden, um eine Sicherung der Kerneldaten bei jedem Windows-Start durchzuführen.

   Stellen Sie sicher, dass die Computer vor dem dritten Neustart nicht in den Ruhezustand versetzt werden, damit die Sicherung der Kerneldaten erfolgreich abgeschlossen werden kann.

SafeGuard Enterprise wird auf dem Endpoint eingerichtet. Informationen zum Anmeldeverhalten des Computers nach der Installation von SafeGuard Enterprise finden Sie in der *SafeGuard Enterprise Benutzerhilfe*.

9.5.3 Zentrale Installation der Verschlüsselungssoftware

Durch die zentrale Installation der Verschlüsselungssoftware wird eine standardisierte Installation auf mehreren Endpoints erreicht.

Hinweis: Die Installations- und Konfigurationspakete können im Rahmen einer zentralen Softwareverteilung nur einem Endpoint zugewiesen werden, nicht aber einem Benutzer.

So führen Sie eine zentrale Installation durch:

- Prüfen Sie die verfügbaren Installationspakete und Features für zentral verwaltete Endpoints und Standalone-Endpoints, siehe *Installationspakete und Features* (Seite 57).
- Prüfen Sie die Kommandozeilenoptionen.
- Prüfen Sie die Liste mit Feature-Parametern für die ADDLOCAL Befehlszeilenoption.
- Prüfen Sie die Beispielbefehle.
- Bereiten Sie das Installationsskript vor.

9.5.3.1 Zentrale Installation der Verschlüsselungssoftware über Active Directory

Stellen Sie sicher, dass Sie die folgenden Schritte bei der zentralen Installation der Verschlüsselungssoftware über Gruppenrichtlinienobjekte (GPO) in einem Active Directory durchführen:

Hinweis: Die Installations- und Konfigurationspakete können im Rahmen einer zentralen Softwareverteilung nur einem Endpoint zugewiesen werden, nicht aber einem Benutzer.

- Verwenden Sie ein gesondertes Gruppenrichtlinienobjekt (GPO) für jedes Installationspaket und sortieren Sie sie in der folgenden Reihenfolge:

  Kompatibilitätskomponente
  Prä-Installationspaket
  Verschlüsselungssoftware-Paket
  Endpoint-Konfigurationspaket

  Für weitere Informationen zur den Paketen, siehe *Vorbereiten des Installationsskripts* (Seite 61).

- Wenn die Sprache des Endpoints nicht auf Deutsch gestellt ist, führen Sie zusätzlich folgendes aus: Wählen Sie im Gruppenrichtlinien-Editor das entsprechende Gruppenobjekt aus und wählen Sie dann **Computerkonfiguration** > **Softwareeinstellungen** > **Erweitert**. Wählen Sie im Dialog **Erweiterte Bereitstellungsoptionen Sprache beim Bereitstellen dieses Pakets ignorieren** und klicken Sie **OK**.

9.5.3.2 Vorbereiten des Installationsskripts

Voraussetzungen:

- Die Endpoints müssen für die Verschlüsselung vorbereitet sein.
- Entscheiden Sie, welches Verschlüsselungspaket und welche Features installiert werden sollen.

So führen Sie eine zentrale Installation der Verschlüsselungssoftware durch:

1. Erstellen Sie ein Verzeichnis mit der Bezeichnung **`Software`** als zentralen Speicherort für alle Anwendungen.

2. Verwenden Sie Ihre eigenen Tools, um das Installationspaket zu erstellen, das auf den Endpoints installiert werden soll. Das Paket muss Folgendes in der angegebenen Reihenfolge enthalten:

Paket	Beschreibung
Prä-Installationspaket `SGxClientPreinstall.msi`	Das obligatorische Paket stattet die Endpoints mit den nötigen Voraussetzungen für eine erfolgreiche Installation der aktuellen Verschlüsselungssoftware aus, zum Beispiel mit der benötigten DLL `MSVCR110.dll`. **Hinweis:** Wenn dieses Paket nicht installiert ist, wird die Installation der Verschlüsselungssoftware abgebrochen.
Verschlüsselungssoftware-Paket	Für eine Liste der verfügbaren Pakete, siehe *Installationspakete und Features* (Seite 57).
Konfigurationspaket für Endpoints	Verwenden Sie die zuvor im SafeGuard Management Center erzeugten Konfigurationspakete. Für zentral verwaltete Endpoints und Standalone-Endpoints müssen unterschiedliche Konfigurationspakete installiert werden, siehe *Erzeugen von Konfigurationspaketen* (Seite 53). Löschen Sie zunächst alle veralteten Konfigurationspakete.

3. Erstellen Sie ein Skript mit den Kommandos für die vorkonfigurierte Installation. Im Skript müssen die Features der Verschlüsselungssoftware aufgelistet sein, die Sie installieren möchten, siehe *Feature-Parameter für die ADDLOCAL Option* (Seite 64). Öffnen Sie eine Befehlseingabeaufforderung und geben Sie die Scripting-Befehle ein. Für Informationen zur Kommandozeilen-Syntax, siehe *Kommandozeilenoptionen für die zentrale Installation* (Seite 63).
4. Verteilen Sie das Paket über unternehmensinterne Software-Verteilungsmechanismen an die Endpoints.

   Das Installation wird auf den Endpoints ausgeführt. Danach sind die Endpoints für den Einsatz von SafeGuard Enterprise bereit.

5. Stellen Sie nach der Installation sicher, dass die Endpoints zweimal neu gestartet werden, um die Power-on Authentication zu aktivieren. Die Computer müssen ein drittes Mal neu gestartet werden, um eine Sicherung der Kerneldaten bei jedem Windows-Start durchzuführen.

   Stellen Sie sicher, dass die Computer vor dem dritten Neustart nicht in den Ruhezustand versetzt werden, damit die Sicherung der Kerneldaten erfolgreich abgeschlossen werden kann.

Zusätzliche Konfiguration kann erforderlich sein, damit sich die Power-on Authentication (POA) auf jeder Hardware-Plattform korrekt verhält. Die meisten Hardware-Konflikte lassen sich mit Hilfe von **Hotkeys**-Funktionalitäten beheben, die in die POA integriert sind. Hotkeys können nach der Installation konfiguriert werden, entweder in der POA selbst oder über eine zusätzliche Konfigurationseinstellung, die dem Windows Installer Befehl msiexec mitgegeben wird. Weitere Informationen finden Sie unter:

http://de.sophos.com/support/knowledgebase/107781.aspx

http://de.sophos.com/support/knowledgebase/107785.aspx

9.5.3.3 Kommandozeilenoptionen für die zentrale Installation

Wir empfehlen, für die zentrale Installation ein Skript mit der Windows Installer Komponente **msiexec** zu erstellen. **Msiexec** führt eine vorkonfigurierte SafeGuard Enterprise Installation automatisch aus. **Msiexec** ist in Windows enthalten. Weitere Informationen finden Sie unter: *http://msdn.microsoft.com/en-us/library/aa367988(VS.85).aspx*.

Kommandozeilen-Syntax

```
msiexec /i <path+msi package name> /qn ADDLOCAL=ALL | <SGN
Features> <SGN parameter>
```

Die Kommandozeilensyntax setzt sich folgendermaßen zusammen:

- Windows Installer Parameter, die z. B. Warnungen und Fehlermeldungen während der Installation in eine Datei protokollieren.
- Sophos SafeGuard Features, die installiert werden sollen, z. B. vollständige, volume-basierende Festplattenverschlüsselung.
- Sophos SafeGuard Parameter, die z. B. das Installationsverzeichnis angeben.

Kommandozeilen-Optionen

Alle verfügbaren Optionen können Sie über msiexec.exe in der Eingabeaufforderung abrufen. Im Folgenden sind wichtige Optionen beschrieben.

Option	Beschreibung
/i	Gibt an, dass es sich um eine Installation handelt.
/qn	Installiert ohne Benutzerinteraktion und zeigt keine Benutzeroberfläche an.
ADDLOCAL=	Listet die Sophos SafeGuard Features auf, die installiert werden. Wird die Option nicht angegeben, werden alle Features installiert, die für eine Standardinstallation vorgesehen sind. Eine Liste der Sophos SafeGuard Features in den einzelnen Installationspaketen und Informationen zu deren Verfügbarkeit je nach Endpoint-Konfiguration finden Sie unter *Installationspakete und Features* (Seite 57). Für eine Liste der Feature-Parameter für die ADDLOCAL Option, siehe *Feature-Parameter für die ADDLOCAL Option* (Seite 64).
ADDLOCAL=ALL	Unter Windows 7 installiert **ADDLOCAL=ALL** die SafeGuard volume-basierende Verschlüsselung und alle anderen verfügbaren Module. Unter Windows 8 installiert **ADDLOCAL=ALL** BitLocker Unterstützung ohne Challenge/Response und alle anderen verfügbaren Module.

Option	Beschreibung
REBOOT=Force | ReallySuppress	Erzwingt oder unterdrückt einen Neustart nach der Installation. Ohne Angabe wird der Neustart erzwungen (Force).
/L* <path + filename>	Protokolliert alle Warnungen und Fehlermeldungen in die angegebene Protokolldatei. Der Parameter **/Le <Pfad + Dateiname>** protokolliert ausschließlich Fehlermeldungen.
Installdir= <Verzeichnis>	Gibt das Verzeichnis an, in das die SafeGuard Enterprise Verschlüsselungssoftware installiert werden soll. Ohne Angabe wird als Standardinstallationsverzeichnis <SYSTEM>:\PROGRAMME\SOPHOS verwendet.

9.5.3.4 Feature-Parameter für die ADDLOCAL Option

Sie müssen Sie bereits im Vorfeld definieren, welche Features auf den Endpoints installiert werden sollen. Die Feature-Namen werden als Parameter zur Kommandozeilenoption ADDLOCAL hinzugefügt. Listen Sie die Features nach der Eingabe der Option **ADDLOCAL** auf:

- Trennen Sie die Features durch Kommas, nicht durch Leerzeichen.
- Achten Sie außerdem auf die Groß-/Kleinschreibung.
- Wenn Sie ein Feature auswählen, müssen Sie auch alle übergeordneten Features (Feature Parents) zur Kommandozeile hinzufügen.
- Sie müssen das Feature **Client** standardmäßig auflisten.

In den folgenden Tabellen sind alle Features aufgelistet, die auf den Endpoints installiert werden können. Weitere Informationen finden Sie unter: *http://www.sophos.com/de-de/support/knowledgebase/108426.aspx*.

9.5.3.4.1 Features für die Sophos SafeGuard Festplattenverschlüsselung

In der folgenden Tabelle sind die für das Paket für die Sophos SafeGuard Festplattenverschlüsselung von (SGNClient.msi, SGNClient_x64.msi) verfügbaren Features aufgelistet, die zur ADDLOCAL Option hinzugefügt werden können.

Hinweis: Sie müssen das Feature **Client** standardmäßig angeben.

Feature Parents	Feature
Client	**CredentialProvider** Obligatorisch Das Feature dient zur Anmeldung über den Credential Provider.
Client,BaseEncryption	**SectorBasedEncryption** Festplattenverschlüsselung

Feature Parents	Feature
	Hinweis: Es kann entweder **SectorBasedEncryption** ODER **BitLockerSupport** angegeben werden.
Client,BaseEncryption	**BitLockerSupport**
Client,BaseEncryption,BitLockerSupport	**BitLockerSupportCR**

9.5.3.4.2 Features für die dateibasierende Verschlüsselung

In der folgenden Tabelle sind die für das Paket für die dateibasierende Verschlüsselung (SGNClient_withoutDE.msi, SGNClient_withoutDE_x64.msi) verfügbaren Features aufgelistet, die zur ADDLOCAL Option hinzugefügt werden können.

Hinweis: Sie müssen das Feature **Client** standardmäßig angeben.

Feature Parents	Feature
Client	**CredentialProvider** Obligatorisch Das Feature dient zur Anmeldung über den Credential Provider.
Client	**SecureDataExchange**
Client	**FileShare**
Client	**CloudStorage**

9.5.3.5 Beispielbefehl: SafeGuard Festplattenverschlüsselung mit File Share

Folgendes wird durch den Befehl installiert:

- Die Endpoints werden mit den notwendigen Voraussetzungen für eine erfolgreiche Installation der aktuellen Verschlüsselungssoftware ausgestattet.
- Anmeldung an die Endpoints mit dem Windows 7 Credential Provider.
- SafeGuard Enterprise Power-on Authentication (POA)
- SafeGuard Enterprise Festplattenverschlüsselung (volume-basierend)
- SafeGuard File Share mit dateibasierender Verschlüsselung von Daten auf der lokalen Festplatte und auf Netzwerkfreigaben
- Das Konfigurationspaket, das den Endpoint als zentral verwalteten Endpoint konfiguriert und eine Verbindung zum SafeGuard Enterprise Server ermöglicht.
- Log-Dateien werden erzeugt.

Beispielbefehl:

```
msiexec /i F:\Software\SGxClientPreinstall.msi /qn /log
I:\Temp\SGxClientPreinstall.log
```

```
msiexec /i F:\Software\SGNClient.msi /qn /log
I:\Temp\SGNClient.log
ADDLOCAL=Client,CredentialProvider,BaseEncryption,SectorBasedEncryption,FileShare
 Installdir=C:\Program Files\Sophos\SafeGuard Enterprise
```

```
msiexec /i F:\Software\SGNConfig_managed.msi /qn /log
I:\Temp\SGNConfig_managed.log
```

9.5.3.6 Beispielbefehl: Dateibasierende Verschlüsselung

Folgendes wird durch den Befehl installiert:

- Die Endpoints werden mit den notwendigen Voraussetzungen für eine erfolgreiche Installation der aktuellen Verschlüsselungssoftware ausgestattet.
- SafeGuard Data Exchange mit dateibasierender Verschlüsselung von Daten auf Wechselmedien
- SafeGuard File Share mit dateibasierender Verschlüsselung von Daten auf der lokalen Festplatte und auf Netzwerkfreigaben
- SafeGuard Cloud Storage mit dateibasierender Verschlüsselung von Daten in der Cloud.
- Das Konfigurationspaket, das den Endpoint als zentral verwalteten Endpoint konfiguriert und eine Verbindung zum SafeGuard Enterprise Server ermöglicht.
- Log-Dateien werden erzeugt.

Beispielbefehl:

```
msiexec /i F:\Software\SGxClientPreinstall.msi /qn /log
I:\Temp\SGxClientPreinstall.log
```

```
msiexec /i F:\Software\SGNClient_withoutDE.msi /qn /log
I:\Temp\SGNClient_withoutDE.log
```

```
ADDLOCAL=Client,CredentialProvider,SecureDataExchange,FileShare,CloudStorage
 Installdir=C:\Program Files\Sophos\SafeGuard Enterprise
```

```
msiexec /i F:\Software\SGNConfig_managed.msi /qn /log
I:\Temp\SGNConfig_managed.log
```

9.5.3.7 Beispielbefehl: SafeGuard BitLocker mit Challenge/Response und File Share

Folgendes wird durch den Befehl installiert:

- Die Endpoints werden mit den notwendigen Voraussetzungen für eine erfolgreiche Installation der aktuellen Verschlüsselungssoftware ausgestattet.
- Anmeldung an die Endpoints mit dem Windows 7 Credential Provider.
- SafeGuard BitLocker Unterstützung.
- SafeGuard Challenge/Response für BitLocker Recovery.
- SafeGuard File Share mit dateibasierender Verschlüsselung von Daten auf der lokalen Festplatte und auf Netzwerkfreigaben
- Das Konfigurationspaket, das den Endpoint als zentral verwalteten Endpoint konfiguriert und eine Verbindung zum SafeGuard Enterprise Server ermöglicht.
- Log-Dateien werden erzeugt.

Beispielbefehl:

```
msiexec /i F:\Software\SGxClientPreinstall.msi /qn /log
I:\Temp\SGxClientPreinstall.log
```

```
msiexec /i F:\Software\SGNClient.msi /qn /log
I:\Temp\SGNClient.log
ADDLOCAL=Client,BaseEncryption,CredentialProvider,BitLockerSupport,BitLockerSupportCR,FileShare
 Installdir=C:\Program Files\Sophos\SafeGuard Enterprise
```

```
msiexec /i F:\Software\SGNConfig_managed.msi /qn /log
I:\Temp\SGNConfig_managed.log
```

9.5.4 Feature-Parameter für die Aktualisierung

Allgemein wird die Aktualisierung der Endpoint Software auf die gleiche Art durchgeführt wie eine zentrale Installation.

Es gelten die folgenden Einschränkungen:

- Der Modus der Festplattenverschlüsselung (SafeGuard volume-basierende Verschlüsselung versus BitLocker Verschlüsselung) kann während einer Aktualisierung nicht geändert werden. Falls Sie den Modus der Festplattenverschlüsselung ändern wollen, müssen Sie die Endpoint Software zunächst deinstallieren und dann die neue Version installieren.
- Ein Wechsel von BitLocker zu BitLocker mit Challenge/Response oder umgekehrt ist nicht möglich. Falls Sie den Modus der BitLocker Unterstützung ändern wollen, müssen Sie die Endpoint Software zunächst deinstallieren und dann die gewünschte Version installieren.
- Unter Windows 7 installiert **ADDLOCAL=ALL** die SafeGuard volume-basierende Verschlüsselung
- Unter Windows 8 installiert **ADDLOCAL=ALL** BitLocker Unterstützung ohne Challenge/Response.

9.6 Lokales Installieren der Verschlüsselungssoftware für Mac

1. Gehen Sie mit der Web-Adresse und den Download-Anmeldedaten auf die Sophos Website und laden Sie den Sophos SafeGuard Disk Encryption Installer for Mac OS X herunter.
2. Suchen Sie im Download-Ordner nach dem Installer Disk Image. Öffnen Sie das Image. Suchen Sie Sophos SafeGuard.pkg und klicken Sie auf dem Paket doppelt, um den Installer zu starten.
3. Klicken Sie auf **Weiter**. Führen Sie die angegebenen Handlungsschritte aus.
4. Geben Sie die Mac OS X Administratoranmeldedaten ein, wenn Sie der Installer dazu auffordert. Dies ist notwendig, damit der Installer Änderungen vornehmen kann.
5. Wenn der Installer abgeschlossen ist, starten Sie Ihren Mac neu.
6. Nach dem Neustart ist Sophos SafeGuard Disk Encryption installiert.
7. Die Power-on Authentication ist noch nicht aktiviert. Es wird jedoch "Secured by SOPHOS" angezeigt. Nach etwa einer Sekunde wird das Betriebssystem gestartet. Solange noch kein SafeGuard Benutzer vorhanden ist, zeigt die Software weiterhin "Secured by SOPHOS" an. Wenn der erste Benutzer erstellt wird, wird die Power-on Authentication aktiviert.

Sophos SafeGuard Disk Encryption for Mac platziert ein Symbol auf die rechte Seite der Menüleiste. Durch Klicken auf dieses Symbol erhalten Sie Zugriff auf die Sophos SafeGuard Disk Encryption Benutzer- und Disk-Verwaltungsfunktionen.

Deinstallation von Sophos SafeGuard Disk Encryption for Mac

Um Sophos SafeGuard Disk Encryption zu deinstallieren, verwenden Sie das Uninstaller Package **Sophos SafeGuard Uninstaller.pkg aus /Library/Sophos SafeGuard.** Sie müssen zunächst die Festplatte entschlüsseln.

9.7 Installation gemäß FIPS

Die FIPS-Zertifizierung beschreibt Sicherheitsanforderungen für Verschlüsselungsmodule. So stellen z. B. Behörden in den USA und in Kanada an Software für besonders sicherheitskritische Informationen die Anforderung der FIPS 140-2 Zertifizierung.

SafeGuard Enterprise nutzt FIPS-zertifizierte AES-Algorithmen. Standardmäßig wird eine neue, schnellere Implementierung der AES-Algorithmen installiert, die noch nicht FIPS-zertifiziert ist.

Um die FIPS-zertifizierte Variante des AES-Algorithmus zu nutzen, setzen Sie beim Installieren der SafeGuard Enterprise Verschlüsselungssoftware die Eigenschaft FIPS_AES auf 1 (eins).

Das machen Sie, indem Sie die Eigenschaft zum Kommandozeilen-Skript hinzufügen:

```
msiexec /i F:\Software\SGNClient.msi FIPS=1
```

Hinweis: Dies betrifft nur SafeGuard Enterprise Device Encryption und Windows 7.

Hinweis: Wenn Sie eine FIPS-konforme Installation aktualisieren, beachten Sie bitte, dass die neuen Versionen ebenfalls gemäß FIPS installiert werden, unabhängig davon, welche Einstellung Sie wählen.

9.8 Installation auf selbst-verschlüsselnden Opal-Festplatten

SafeGuard Enterprise unterstützt den anbieter-unabhängigen Opal-Standard für selbst-verschlüsselnde Festplatten und bietet die Verwaltung von Endpoints mit dieser Art von Festplatten.

Um sicherzustellen, dass die Unterstützung von selbst-verschlüsselnden Opal-Festplatten diesem Standard möglichst genau entspricht, werden bei der Installation von SafeGuard Enterprise auf dem Endpoint zwei Arten von Prüfungen durchgeführt:

- **Funktionale Prüfungen**

  Hier wird u. a. geprüft, ob sich die Festplatte als "OPAL"-Festplatte identifiziert, ob Kommunikationseinstellungen korrekt sind und ob alle für SafeGuard Enterprise erforderlichen Opal Features von der Festplatte unterstützt werden.

- **Sicherheitsprüfungen**

  Mit Sicherheitsprüfungen wird sichergestellt, dass nur SafeGuard Enterprise Benutzer auf der Festplatte registriert sind und dass nur SafeGuard Enterprise Benutzer die Schlüssel für die software-basierende Verschlüsselung von nicht selbst-verschlüsselnden Laufwerken haben. Wird bei der Installation festgestellt, dass andere Benutzer registriert sind, versucht SafeGuard Enterprise automatisch, diese zu deaktivieren. Diese Funktionalität wird durch den Opal-Standard gefordert. Ausgenommen sind hier einige wenige Standard "Authorities", die für den Betrieb eines Opal-Systems erforderlich sind.

  Hinweis: Diese Sicherheitsprüfungen werden wiederholt, wenn nach einer erfolgreichen Installation im Opal-Modus eine Verschlüsselungsrichtlinie für die Festplatte angewendet wird. Schlagen die Sicherheitsprüfungen in diesem Fall fehl, so haben inzwischen außerhalb von SafeGuard Enterprise Eingriffe in die Laufwerksverwaltung stattgefunden. In diesem Fall verweigert SafeGuard Enterprise den Zugriff auf das Laufwerk und es wird eine entsprechende Meldung angezeigt.

Sollten einige dieser Prüfungen ohne Recovery-Möglichkeit fehlschlagen, so wird für die Installation nicht die software-basierende Verschlüsselung angewendet. Stattdessen bleiben alle Volumes auf der Opal-Festplatte unverschlüsselt.

Wenn Sie erzwingen möchten, dass keine Opal-Prüfungen durchgeführt werden, verwenden Sie folgende Kommandozeilensyntax:

```
MSIEXEC /i <name_of_selected_client_msi>.msi OPALMODE=2
```

Bei einigen Opal-Festplatten bestehen u. U. Sicherheitsprobleme. Es besteht keine Möglichkeit, automatisch festzustellen, welche Privilegien unbekannten Benutzern/Authorities zugeordnet sind, die bereits zum Zeitpunkt der SafeGuard Enterprise Installation/Verschlüsselung registriert waren. Wenn die Festplatte den Befehl, diese Benutzer zu deaktivieren, nicht ausführt, wendet SafeGuard Enterprise die software-basierende Verschlüsselung an, um die größtmögliche Sicherheit für den SafeGuard Enterprise Benutzer zu gewährleisten. Da wir für die Festplatten selbst keine Sicherheitsgarantien geben können, haben wir einen speziellen Installationsschalter implementiert. Diesen Schalter können Sie verwenden, um Festplatten mit potentiellen Sicherheitsrisiken auf eigene Verantwortung zu benutzen. Eine Liste der Festplatten, für die dieser Schalter erforderlich ist, sowie weitere Informationen zu unterstützten Festplatten finden Sie in den SafeGuard Enterprise Release Notes.

Um den Installationsschalter anzuwenden, benutzen Sie folgende Kommandozeilensyntax:

```
MSIEXEC /i <name_of_selected_client_msi>.msi
IGNORE_OPAL_AUTHORITYCHECK_RESULTS=1
```

Wenn Sie die Installation mit einem Transform durchführen möchten: Die interne Eigenschaft der .msi-Datei hat denselben Namen.

Weitere Informationen zu SafeGuard Enterprise in Kombination mit Opal-Festplatten finden Sie in der *SafeGuard Enterprise Administratorhilfe* und *Benutzerhilfe*.

10 Einrichten von SafeGuard Enterprise Runtime

Die SafeGuard Enterprise Verschlüsselungssoftware kann auch dann zum Schutz der Daten installiert werden, wenn mehrere Betriebssysteme auf separaten Volumes der Endpoint-Festplatte (Runtime-System) installiert sind. SafeGuard Enterprise Runtime stellt folgende Sachverhalte sicher, wenn die Software auf Volumes mit einer zusätzlichen Windows-Installation installiert wird:

- Die Windows-Installation, die sich auf diesen Volumes befindet, kann erfolgreich durch einen Boot Manager gestartet werden.
- Auf Partitionen auf diesen Volumes, die durch eine vollständige SafeGuard Enterprise Client Installation mit dem definierten Computerschlüssel verschlüsselt worden sind, kann erfolgreich zugegriffen werden.

10.1 Voraussetzungen und Einschränkungen

Beachten Sie:

- SafeGuard Enterprise Runtime bietet keine SafeGuard Enterprise Verschlüsselungs-Features oder Funktionalitäten.
- SafeGuard Enterprise Runtime unterstützt nur die Betriebssysteme, die auch für die SafeGuard Enterprise Verschlüsselungssoftware unterstützt werden.
- USB-Tastaturen können u. U. nur eingeschränkt benutzt werden.
- Es werden nur Boot Manager unterstützt, die nach der Power-on Authentication aktiv werden.
- Die Unterstützung von Boot Managern von Drittanbietern wird nicht garantiert. Wir empfehlen den Einsatz von Microsoft Boot Managern.
- SafeGuard Enterprise Runtime kann nicht auf eine SafeGuard Enterprise Verschlüsselungsinstallation in Vollversion aktualisiert werden.
- Das Runtime-Installationspaket muss vor der Installation der Vollversion des Enterprise Verschlüsselungspakets installiert werden.
- Es kann nur auf Volumes, die mit dem definierten Computerschlüssel in SafeGuard Enterprise verschlüsselt wurden, zugegriffen werden.

10.2 Vorbereitung

Um SafeGuard Enterprise Runtime einzurichten, führen Sie die folgenden vorbereitenden Schritte in der angegebenen Reihenfolge durch:

1. Stellen Sie sicher, dass die Volumes, auf denen SafeGuard Enterprise Runtime laufen soll, zum Zeitpunkt der Installation sichtbar sind und mit ihrem Windows-Namen (z. B. C:) angesprochen werden können.
2. Legen Sie fest, auf welchem Volume/welchen Volumes der Festplatte SafeGuard Enterprise Runtime installiert werden soll. In Zusammenhang mit SafeGuard Enterprise sind diese Volumes als "sekundäre" Windows-Installationen definiert. Es können mehrere sekundäre Windows-Installationen vorhanden sein. Verwenden Sie folgendes Paket: SGNClientRuntime.msi oder SGNClientRuntime_x64.msi (unter Windows 64 Bit).
3. Legen Sie fest, auf welchem Volume der Festplatte die Vollversion des SafeGuard Enterprise Clients installiert werden soll. In Zusammenhang mit SafeGuard Enterprise ist dieses Volume als “primäre“ Windows-Installation definiert. Es kann jeweils nur eine primäre Windows-Installation geben. Verwenden Sie folgendes Paket: SGNClientRuntime.msi oder SGNClientRuntime_x64.msi (unter Windows 64 Bit).
4. Bereiten Sie die Computer für die Verschlüsselung vor, siehe *Vorbereiten der Endpoints für die Verschlüsselung* (Seite 51).

10.3 Installieren von SafeGuard Runtime

1. Wählen Sie das/die gewünschte(n) sekundäre(n) Volume(s) der Festplatte aus, auf dem/denen Sie SafeGuard Enterprise Runtime Client installieren möchten.
2. Starten Sie die sekundäre Windows-Installation auf dem ausgewählten Volume.
3. Installieren Sie das Runtime-Installationspaket auf dem ausgewählten Volume.
4. Übernehmen Sie die Standardeinstellungen im nächsten Dialog des Installers. Sie müssen keine speziellen Features auswählen.
5. Wählen Sie einen Installationsordner für die Runtime-Installation.
6. Klicken Sie auf **Beenden**, um die Runtime-Installation abzuschließen.
7. Wählen Sie das primäre Volume der Festplatte, auf dem Sie die SafeGuard Enterprise Verschlüsselungssoftware installieren möchten.
8. Starten Sie die primäre Windows-Installation auf dem ausgewählten Volume.
9. Starten Sie das Prä-Installationspaket SGxClientPreinstall.msi. Dieses Paket stattet die Endpoints mit notwendigen Voraussetzungen für die erfolgreiche Installation der Verschlüsselungssoftware aus.
10. Installieren Sie das SafeGuard Enterprise Verschlüsselungspaket auf dem ausgewählten Volume.
11. Erstellen Sie ein Konfigurationspaket gemäß Ihren Anforderungen und verteilen Sie es an den Endpoint.
12. Verschlüsseln Sie beide Volumes mit dem definierten Computerschlüssel.

10.4 Starten von einem sekundären Volume über einen Boot Manager

1. Starten Sie den Computer.
2. Melden Sie sich an der Power-on Authentication mit Ihren Anmeldeinformationen an.
3. Starten Sie den Boot Manager und wählen Sie das gewünschte sekundäre Volume als Boot-Laufwerk.
4. Starten Sie den Computer von diesem Volume neu.

Auf jedes Volume, das mit dem definierten Computerschlüssel verschlüsselt ist, kann zugegriffen werden.

11 Replikation der SafeGuard Enterprise Datenbank

Zur Optimierung der Performance der SafeGuard Enterprise Datenbank lässt sich diese auf mehrere SQL Server replizieren.

Dieser Abschnitt beschreibt das Aufsetzen der Replikation für die SafeGuard Enterprise Datenbank in einer verteilten Umgebung. In der Beschreibung wird davon ausgegangen, dass Sie bereits Erfahrung mit dem Microsoft SQL Server Replikationsmechanismus haben.

Hinweis: Die Administration sollte nur bei der Master-Datenbank erfolgen, nicht bei replizierten Datenbanken.

11.1 Mergereplikation

Die Mergereplikation ist der Vorgang der Verteilung von Daten vom Verleger an die Abonnenten. Dabei können Verleger und Abonnenten unabhängig voneinander Aktualisierungen vornehmen und danach einen Merge der Aktualisierungen zwischen den Standorten durchführen.

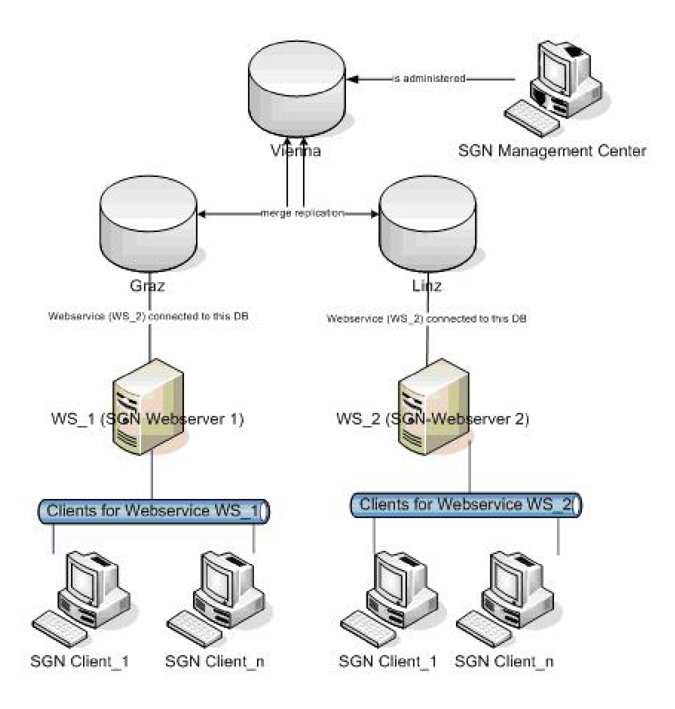
Die Mergereplikation erlaubt es verschiedenen Standorten, autonom zu arbeiten und später die Aktualisierungen zu einem einzigen, einheitlichen Ergebnis zusammenzuführen. Der initiale Snapshot wird auf die Abonnenten angewendet. Microsoft SQL Server verfolgt dann die Änderungen an veröffentlichten Daten beim Verleger und bei den Abonnenten nach. Die Daten werden zwischen den Servern kontinuierlich, zu einem festgelegten Zeitpunkt oder auf Anforderung synchronisiert. Da Aktualisierungen auf mehr als einem Server ausgeführt werden, sind dieselben Daten möglicherweise vom Verleger und von mindestens einem Abonnenten aktualisiert worden. Daher kann es beim Zusammenführen von Aktualisierungen zu Konflikten kommen.

Die Mergereplikation bietet Standardmöglichkeiten sowie individuelle Möglichkeiten für die Konfliktlösung, die Sie bei der Konfiguration einer Mergeveröffentlichung definieren können. Tritt ein Konflikt auf, ruft der Merge-Agent einen Resolver auf. Dieser bestimmt, welche Daten akzeptiert und an andere Standorte verteilt werden.

11.2 Einrichten der Datenbankreplikation

Der Vorgang des Einrichtens einer Replikation für die SafeGuard Enterprise Datenbank wird am Beispiel von Microsoft SQL Server 2005 beschrieben.

Im Beispiel wird SafeGuard Enterprise ausschließlich von der Datenbank in **Wien** aus administriert. Alle Änderungen werden vom SafeGuard Management Center über den Microsoft SQL Server 2005 Replikationsmechanismus an die Datenbanken in **Graz** und **Linz** weitergegeben. Die von den Client-Computern über die Web Server gemeldeten Änderungen werden ebenfalls über den Replikationsmechanismus an den Microsoft SQL Server 2005 weitergegeben.



11.2.1 Erzeugen der Master-Datenbank

Legen Sie zunächst die SafeGuard Enterprise Master-Datenbank an. In unserem Beispiel ist dies die Datenbank Wien.

Der Vorgang zum Erzeugen der Master-Datenbank ist mit dem entsprechenden Vorgang für eine SafeGuard Enterprise Installation ohne Replikation identisch.

- Erzeugen der Master-Datenbank im SafeGuard Management Center Konfigurationsassistenten.

  Für diesen Vorgang muss das SafeGuard Management Center bereits installiert sein. Für weitere Informationen, siehe *Starten der Erstkonfiguration des SafeGuard Management Centers* (Seite 27).

- Erzeugen Sie die Master-Datenbank mit einem SQL-Skript. Sie finden SQL Skripte in Ihrer Produktlieferung.

  Dieser Vorgang wird häufig bevorzugt, wenn erweiterte SQL-Berechtigungen während der SafeGuard Management Konfiguration nicht erwünscht sind. Für weitere Informationen, siehe *Erzeugen der SafeGuard Enterprise Datenbank per Skript* (Seite 21).

11.2.2 Erzeugen der Replikationsdatenbanken Graz und Linz

Nach dem Einrichten der Master-Datenbank erzeugen Sie die Replikationsdatenbanken. Im Beispiel haben die Replikationsdatenbanken die Bezeichnungen Graz und Linz.

Hinweis: Datentabellen und EVENT-Tabellen werden in getrennten Datenbanken gehalten. Ereigniseinträge werden standardmäßig nicht verkettet, so dass die EVENT-Datenbank zur Erhöhung der Performance auf mehrere SQL Server repliziert werden kann. Wenn

EVENT-Tabellen verkettet werden, können während der Replikation ihrer Datensätze Probleme auftreten.

So erzeugen Sie die Replikationsdatenbanken neu:

1. Erzeugen Sie eine Veröffentlichung für die Master-Datenbank in der Management-Konsole des SQL Servers.

   Eine Veröffentlichung definiert das Daten-Set, das repliziert werden soll.
2. Wählen Sie alle Tabellen, Ansichten und gespeicherten Prozeduren für die Synchronisierung in dieser Veröffentlichung aus.
3. Erstellen Sie die Replikationsdatenbanken, indem Sie ein Abonnement für Graz und ein Abonnement für Linz erzeugen. Die neuen Datenbanken Graz und Linz erscheinen daraufhin in den Abonnements im SQL Konfigurationsassistenten.
4. Schließen Sie den SQL Konfigurationsassistenten. Die Replikationsüberwachung zeigt, ob der Replikationsmechanismus korrekt läuft.
5. Stellen Sie sicher, dass Sie den korrekten Datenbanknamen in der ersten Zeile des SQL Skripts eingeben. Verwenden Sie zum Beispiel **`Graz`** oder **`Linz`**.
6. Erzeugen Sie nochmal die Snapshots mit dem Snapshot Agenten.

Die Replikationsdatenbanken Graz und Linz wurden angelegt.

11.3 Installieren und Registrieren von SafeGuard Enterprise Servern

Um SafeGuard Enterprise Server auf den Web Servern zu installieren, gehen Sie wie folgt vor.

1. Installieren Sie SafeGuard Enterprise Server auf dem Server WS_1.
2. Installieren Sie SafeGuard Enterprise Server auf dem Server WS_2.
3. Registrieren Sie beide Server im SafeGuard Management Center. Im Menü **Extras** klicken Sie auf **Konfigurationspakete**, und dann auf **Server**. Auf der Registerkarte **Server** klicken Sie auf **Hinzufügen**.
4. Sie werden dazu aufgefordert, die Serverzertifikate **`ws_1.cer`** und **`ws_2.cer`** hinzuzufügen. Sie finden die Zertifikate im Ordner **`\Program Files\Sophos\Sophos SafeGuard\MachCert\`**. Die Zertifikate werden benötigt, um die entsprechenden Konfigurationspakete zu erstellen.

Die SafeGuard Enterprise Server sind installiert und registriert.

11.4 Erzeugen der Konfigurationspakete für die Datenbank Graz

Erzeugen Sie die Konfigurationspakete für die Datenbank Graz: ein Paket für Server WS_1 für die Kommunikation mit der Datenbank Graz sowie ein Paket für die Verbindung des SafeGuard Enterprise Clients Graz mit dem Web Service WS_1.

1. Klicken Sie im SafeGuard Management Center im **Extras** Menü auf **Optionen** und dann auf **Datenbank**.
2. Wählen Sie unter **Verbindungseinstellungen** **`WS_1`** als **Datenbankserver** und Graz als **Datenbank auf Server**. Klicken Sie auf **OK**.

3. Klicken Sie im **Extras** Menü auf **Konfigurationspakete...** und dann auf **Server-Pakete**. Wählen Sie den Server **WS_1** , den Ausgabepfad und klicken Sie auf **Konfigurationspaket erstellen**.
4. Wechseln Sie auf die Registerkarte **Pakete für Managed Clients**. Klicken Sie auf **Konfigurationspaket hinzufügen** und geben Sie einen Namen für das Paket ein. Wählen Sie unter **Primärer Server** den korrekten Server, mit dem die SafeGuard Enterprise Clients Graz verbunden werden sollen: **WS_1**. Legen Sie den Ausgabepfad fest und klicken Sie auf **Konfigurationspaket erstellen**.

Die SafeGuard Enterprise Server und Client Konfigurationspakete für die Datenbank Graz werden am definierten Ausgabeort erstellt.

11.5 Erzeugen der Konfigurationspakete für die Datenbank Linz

Sie müssen die Konfigurationspakete für die Datenbank Linz erzeugen: Ein Paket für Server WS_2 für die Kommunikation mit der Datenbank Linz sowie ein Paket für die Verbindung des SafeGuard Enterprise Clients Linz mit dem Web Service WS_2.

1. Klicken Sie im SafeGuard Management Center im **Extras** Menü auf **Optionen** und dann auf **Datenbank**.
2. Wählen Sie unter **Verbindungseinstellungen** **WS_2** als **Datenbankserver** und Linz als **Datenbank auf Server**. Klicken Sie auf **OK**.
3. Klicken Sie im **Extras** Menü auf **Konfigurationspakete...** und dann auf **Server-Pakete**. Wählen Sie den Server **WS_2** , den Ausgabepfad und klicken Sie auf **Konfigurationspaket erstellen**.
4. Wechseln Sie auf die Registerkarte **Pakete für Managed Clients**. Klicken Sie auf **Konfigurationspaket hinzufügen** und geben Sie einen Namen für das Paket ein. Wählen Sie unter **Primärer Server** den korrekten Server, mit dem die SafeGuard Enterprise Clients Linz verbunden werden sollen: **WS_2**. Legen Sie den Ausgabepfad fest und klicken Sie auf **Konfigurationspaket erstellen**. Klicken Sie auf **Schließen**.
5. Verbinden Sie das SafeGuard Management Center wieder mit der Datenbank Wien: Klicken Sie im **Extras** Menü auf **Optionen** und dann auf **Datenbank**.

Die SafeGuard Enterprise Server und Client Konfigurationspakete für die Datenbank Linz werden am definierten Ausgabeort erstellt.

11.6 Installieren der SafeGuard Enterprise Server Konfigurationspakete

1. Installieren Sie das Server-Konfigurationspaket (**ws_1.msi**) auf Web Service WS_1, der mit der Datenbank Graz kommunizieren soll.
2. Installieren Sie das Server-Konfigurationspaket **ws_2.msi** auf Web Service WS_2, der mit der Datenbank Linz kommunizieren soll.
3. Testen Sie die Kommunikation zwischen den SafeGuard Enterprise Servern und diesen Datenbanken, siehe *Testen der Verbindung (IIS 6 auf Windows Server 2003)*.

11.7 Einrichten des Endpoint

Für Informationen zum Installieren der Verschlüsselungssoftware auf Endpoints, siehe *Zentrale Installation der Verschlüsselungssoftware* (Seite 60).

Hinweis: Stellen Sie zum Einrichten der Endpoints sicher, dass Sie nach der Installation das korrekte Konfigurationspaket installieren:

1. Installieren Sie das Client-Konfigurationspaket Graz auf den Endpoints, die mit dem Graz Server WS_1 verbunden werden sollen.
2. Installieren Sie das Client-Konfigurationspaket Linz auf den Endpoints, die mit dem Linz Server WS_2 verbunden werden sollen.

Weitere Informationen zur Aktualisierung replizierter SafeGuard Enterprise Databanken finden Sie in der *SafeGuard Enterprise Upgrade-Anleitung*.

12 Deinstallation - Überblick

Dieser Abschnitt behandelt folgende Themen:

- Best Practices für die Deinstallation
- Deinstallation der Sophos SafeGuard Verschlüsselungssoftware
- Verhindern der Deinstallation der Sophos SafeGuard Verschlüsselungssoftware.

12.1 Best Practices für die Deinstallation

Wenn die SafeGuard Enterprise Verschlüsselungssoftware auf demselben Computer wie das SafeGuard Management Center installiert ist, führen Sie den folgende Deinstallationsvorgang durch, damit Sie weiterhin eine der beiden Komponenten benutzen können:

1. Deinstallieren Sie das SafeGuard Management Center.
2. Deinstallieren Sie das Konfigurationspaket.
3. Deinstallieren Sie die Verschlüsselungssoftware.
4. Installieren Sie das Paket, das Sie weiterhin benutzen möchten, neu.

12.2 Deinstallation der SafeGuard Enterprise Verschlüsselungssoftware

Führen Sie zum Deinstallieren der SafeGuard Enterprise Verschlüsselungssoftware folgende Schritte durch:

- Entschlüsseln Sie verschlüsselte Daten.
- Deinstallieren Sie die Verschlüsselungssoftware.

  Damit Entschlüsselung und Deinstallation möglich sind, müssen auf den Endpoints die entsprechenden Richtlinien wirksam sein.

12.2.1 Verhindern einer Deinstallation auf den Endpoints

Um den Schutz für Endpoints noch zu verstärken, empfehlen wir, dass Sie die lokale Deinstallation von SafeGuard Enterprise auf Endpoints verhindern. Setzen Sie das Feld **Deinstallation erlaubt** in einer **Spezifische Computereinstellungen** Richtlinie auf **Nein** und übermitteln Sie die Richtlinie an die Endpoints. Versuche, die Software zu deinstallieren, werden daraufhin abgebrochen und die nicht autorisierten Versuche werden protokolliert.

12.2.2 Entschlüsseln von verschlüsselten Daten

Folgende Voraussetzung muss erfüllt sein:

Für die Entschlüsselung von verschlüsselten Volumes müssen alle volume-basierend verschlüsselten Volumes einen Laufwerksbuchstaben haben.

1. Bearbeiten Sie im SafeGuard Management Center die aktuelle Richtlinie vom Typ **Geräteschutz**, den den zu entschlüsselnden Computern zugewiesen ist. Wählen Sie die Ziele und stellen Sie die Option **Benutzer darf Volume entschlüsseln** auf **Ja** ein. Weisen Sie die Richtlinie den relevanten Endpoints zu.
2. Erstellen Sie eine Richtlinie vom Typ **Geräteschutz**, wählen Sie die Ziele, die entschlüsselt werden sollen und stellen Sie den **Verschlüsselungsmodus für Medien** auf **Keine Verschlüsselung** ein.
3. Legen Sie unter **Benutzer & Computer** eine Gruppe für die Computer an, die Sie entschlüsseln möchten: Rechtsklicken Sie auf den Domänenkonten, an dem Sie die Gruppe erstellen möchten. Wählen Sie dann **Neu** > **Neue Gruppe erzeugen**.
4. Wählen Sie den Domänenknoten dieser Gruppe und weisen Sie die Entschlüsselungsrichttlinie zu, indem Sie die Richtlinie aus der **Verfügbare Richtlinien** Liste in die Registerkarte **Richtlinien** ziehen. Aktivieren Sie die Richtlinie, indem Sie jetzt die Gruppe aus der Liste der **Verfügbaren Gruppen** in den Bereich **Aktivierung** ziehen. Stellen Sie in der Registerkarte **Richtlinien** des Domänenknotens sicher, dass die **Priorität** auf 1 gesetzt und die Einstellung **Kein Überschreiben** aktiviert ist. Stellen Sie im Bereich **Aktivierung** des Domänenknotens sicher, dass nur Mitglieder der Gruppe von dieser Richtlinie betroffen sind.
5. Wählen Sie im **Benutzer & Computer** Navigationsbereich die Gruppe, rechtsklicken Sie auf die im Aktionsbereich angezeigte **Mitglieder** Registerkarte und klicken Sie auf **Hinzufügen**, um die Computer, die Sie entschlüsseln möchten, zur Gruppe hinzuzufügen.
6. Führen Sie auf dem Endpoint, der entschlüsselt werden soll, eine Synchronisierung mit dem SafeGuard Enterprise Server durch. Damit stellen Sie sicher, dass die Richtlinienaktualisierung auf dem Computer eingegangen und aktiv ist.
7. Öffnen Sie den Windows Explorer. Klicken Sie mit der rechten Maustaste auf das Volume, das entschlüsselt werden soll, und klicken Sie dann auf **Verschlüsselung** > **Entschlüsselung**.

   Stellen Sie sicher, dass die Verschlüsselung erfolgreich abgeschlossen werden konnte.

   Hinweis: Endpoints können während der Verschlüsselung/Entschlüsselung heruntergefahren und neu gestartet werden. Wenn auf die Entschlüsselung die Deinstallation folgt, empfehlen wir, den Endpoint nicht in einen Energiesparmodus oder den Ruhezustand zu versetzen.

12.2.3 Starten der Deinstallation

Folgende Voraussetzungen müssen erfüllt sein:

- Verschlüsselte Daten müssen korrekt entschlüsselt werden, damit nach der Deinstallation Zugriff auf die Daten besteht. Der Entschlüsselungsvorgang muss abgeschlossen sein. Die korrekte Entschlüsselung ist besonders wichtig, wenn die Deinstallation von Active Directory ausgelöst wird.

  Darüber hinaus müssen vor der Deinstallation des letzten durch SafeGuard Enterprise geschützten Endpoint alle verschlüsselten Wechselmedien entschlüsselt werden. Andernfalls besteht die Gefahr, dass Benutzer nicht mehr auf Ihre Daten zugreifen

können. Solange die SafeGuard Enterprise Datenbank zur Verfügung steht, können die Daten auf den Wechselmedien wiederhergestellt werden.

- Für die Deinstallation der SafeGuard Festplattenverschlüsselung müssen alle volume-basierend verschlüsselten Volumes einen Laufwerksbuchstaben haben.
- Deinstallieren Sie jeweils immer das komplette Paket mit allen installierten Features.

1. Bearbeiten Sie im SafeGuard Management Center die Richtlinie vom Typ **Spezifische Computereinstellungen**. Stellen Sie die Option **Deinstallation erlaubt** auf **Ja** ein.
2. Legen Sie unter **Benutzer & Computer** eine Gruppe für die Computer an, die Sie entschlüsseln möchten: Rechtsklicken Sie auf den Domänenkonten, an dem Sie die Gruppe erstellen möchten. Wählen Sie dann **Neu** > **Neue Gruppe erzeugen**.
3. Wählen Sie den Domänenknoten dieser Gruppe und weisen Sie die Richtlinien zum Deinstallieren zu, indem Sie die Richtlinie aus der **Verfügbare Richtlinien** Liste in die Registerkarte **Richtlinien** ziehen. Aktivieren Sie die Richtlinie, indem Sie jetzt die Gruppe aus der Liste der **Verfügbaren Gruppen** in den Bereich **Aktivierung** ziehen. Stellen Sie in der Registerkarte **Richtlinien** des Domänenknotens sicher, dass die **Priorität** auf 1 gesetzt und die Einstellung **Kein Überschreiben** aktiviert ist. Stellen Sie im Bereich **Aktivierung** des Domänenknotens sicher, dass nur Mitglieder der Gruppe von dieser Richtlinie betroffen sind.
4. Fügen Sie die Endpoints, bei denen die Deinstallation ausgeführt werden soll, zur Gruppe hinzu.
5. Wenden Sie zum Starten der Deinstallation eine der folgenden Methoden an:
   - Um eine lokale Deinstallation auf dem Endpoint durchzuführen, synchronisieren Sie diesen mit dem SafeGuard Enterprise Server. Damit stellen Sie sicher, dass die Richtlinienaktualisierung auf dem Computer eingegangen und aktiv ist. Wählen Sie dann **Start** > **Systemsteuerung** > **Software** > **Sophos SafeGuard Client** > **Entfernen**.
   - Verwenden Sie für eine zentrale Deinstallation einen Software-Verteilungsmechanismus Ihrer Wahl. Stellen Sie sicher, dass alle erforderlichen Daten vor dem Starten der Deinstallation korrekt entschlüsselt wurden.

13 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

- Rufen Sie das SophosTalk-Forum unter *community.sophos.com/* auf und suchen Sie nach Benutzern mit dem gleichen Problem.
- Durchsuchen Sie die Sophos Support-Knowledgebase unter *www.sophos.com/de-de/support.aspx*.
- Laden Sie Produktdokumentation unter *www.sophos.com/de-de/support/documentation/* herunter.
- Senden Sie eine E-Mail an *support@sophos.de* und geben Sie die Versionsnummer(n), Betriebssystem(e) und Patch Level Ihrer Sophos Software sowie ggf. den genauen Wortlaut von Fehlermeldungen an.

14 Rechtliche Hinweise